NXC-8160

Business WLAN Controller

User's Guide

Version 1.0
6/2007
Edition 1

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the NXC-8160 using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide
  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Supporting Disk
  Refer to the included CD for support documents.
- ZyXEL Web Site
  Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The NXC-8160 wireless switch may be referred to as the "NXC-8160", the "WLAN controller" or the "system" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons.

NXC-8160 	Computer 	Notebook computer 
Server 	Wireless Signal 	Modem/Router 
Access Point 		

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Not to remove the plug and plug into a wall outlet by itself; always attach the plug to the power supply first before insert into the wall.
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: RISK OF EXPLOSION IF BATTERY (on the motherboard) IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS. Dispose them at the applicable collection point for the recycling of electrical and electronic equipment. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.

- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

This product is recyclable. Dispose of it properly.

Contents Overview

Table of Contents

List of Figures

List of Tables

PART I
Introduction

1

Getting to Know Your NXC-8160

This chapter introduces the main features and applications of the NXC-8160.

1.1 NXC-8160 Overview

The NXC-8160 is a WLAN controller that allows you to connect the NWA-8500 access points (APs) to extend your wireless network. The NXC-8160 centralizes the management of all of the connected APs. You can maintain the APs through the NXC-8160; thus eliminating the need to connect to and configure each AP individually. The AP acts as an antenna of the NXC-8160.

If you have more than one NXC-8160 in your network, you can manage the other NXC-8160(s) through a NXC-8160. You can also set one NXC-8160 as the main WLAN controller, and the other as the backup when the primary is not active or cannot work properly.

The NXC-8160 provides secure wireless connectivity to your wired network. The NWA-8500 supports two radios (wireless transmissions of signals) simultaneously which can be of the same or different IEEE 802.11 mode. That means both IEEE 802.11b/g and IEEE 802.11a compatible clients can wirelessly access the wired network behind the NXC-8160 through a connected access point.

Only use firmware for your NXC-8160's specific model.

See Chapter 11 on page 81 for a complete list of features.

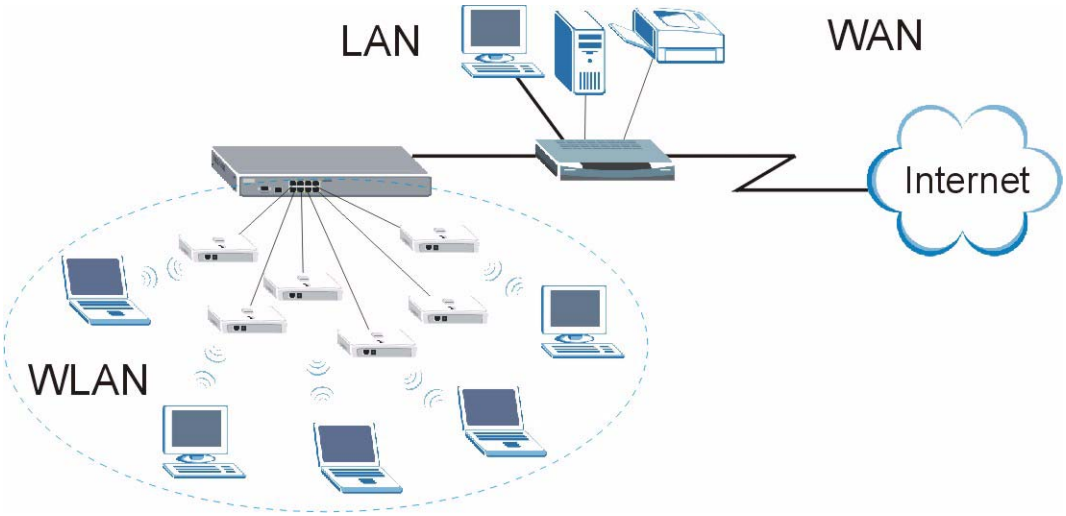
1.2 Application for the NXC-8160

Here are some examples of what you can do with your NXC-8160.

1.2.1 Wireless Internet Access

You can connect a cable or DSL modem/router to the NXC-8160 for broadband Internet access via an Ethernet port on the modem/router. Both IEEE 802.11a or IEEE 802.11 b/g wirless clients can access the network behind the NXC-8160 through the access point(s) connected to the NXC-8160.

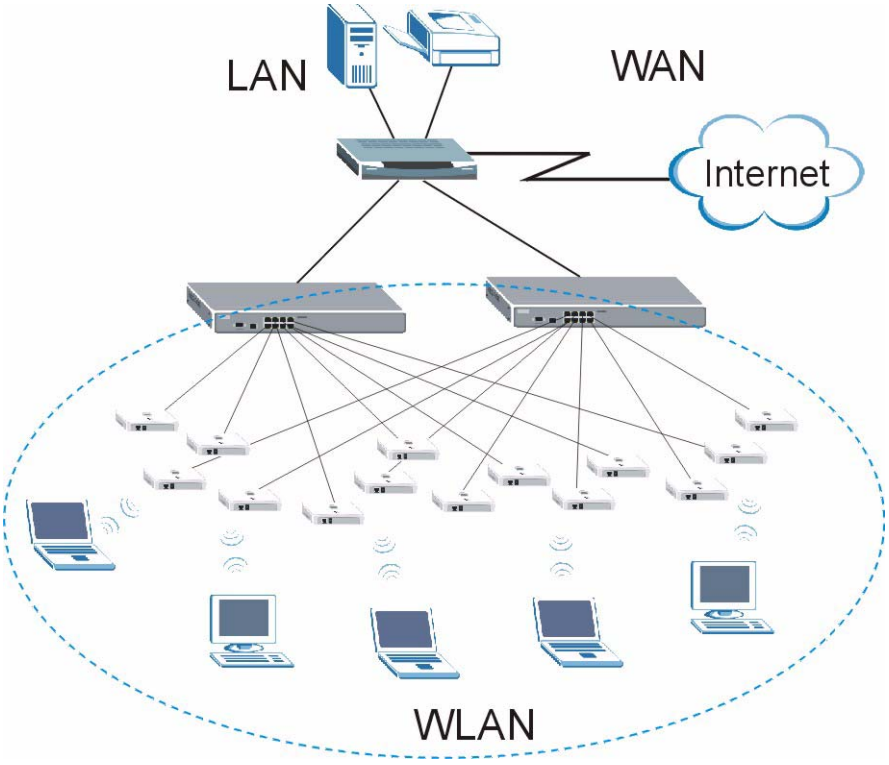
Figure 1 Wireless Internet Access



1.2.2 Backup NXC-8160

To ensure wireless Internet access availability, deploy one NXC-8160 as the main WLAN controller and the other NXC-8160 as the backup. Both NXC-8160s should be in the same network and have the same number of connected access points and use the same wireless settings (such as SSID, channel, IEEE 802.11 mode and security). If the main NXC-8160 fails, wireless clients can still access the Internet or wired network by connecting to the backup NXC-8160.

Figure 2 Backup NXC-8160



1.3 Ways to Manage the NXC-8160

Use any of the following methods to manage the NXC-8160.

- Web Configurator. This is recommended for everyday management of the NXC-8160 using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- SNMP. The device can be monitored by an SNMP manager. See the SNMP chapter in this User's Guide.

1.4 Good Habits for Managing the NXC-8160

Do the following things regularly to make the NXC-8160 more secure and to manage the NXC-8160 more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.

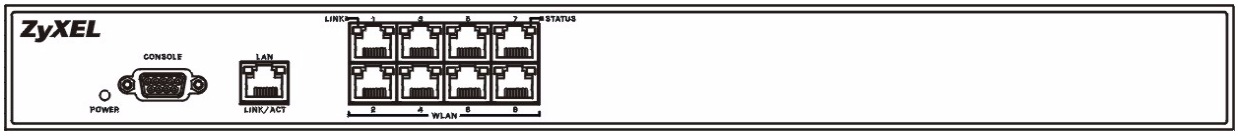
If you forgot the password, you cannot restore the defaults and need to contact your vendor or customer support.

- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you backed up an earlier configuration file, you would not have to totally re-configure the NXC-8160. You could simply restore your last configuration.

1.5 Front Panel LEDs (Lights)

The following figure shows the front panel of the NXC-8160.

Figure 3 Front Panel



The following table describes the lights on the NXC-8160.

Table 1 Front Panel LEDs (Lights)

LED	COLOR	STATUS	DESCRIPTION
POWER		Off	The NXC-8160 is turned off.
	Green	On	The NXC-8160 is ready and running.
		Flashing	The NXC-8160 is restarting.
	Red	On	The power to the NXC-8160 is too low.
LAN			
LINK/ACT		Off	The LAN is not connected.
	Green	On	The NXC-8160 has a successful LAN connection.
		Flashing	The LAN is sending or receiving packets.
WLAN 1 ~ 8			
LINK	Green	Off	The wireless LAN is not ready, or has failed.
		On	The wireless LAN is ready.
		Flashing	The wireless LAN is sending or receiving packets.

2

Introducing the Web Configurator

This chapter describes how to access the NXC-8160 web configurator and provides an overview of its screens.

2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy NXC-8160 setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

See Appendix C on page 119 if you want to make sure these functions are allowed in Internet Explorer or Netscape Navigator.

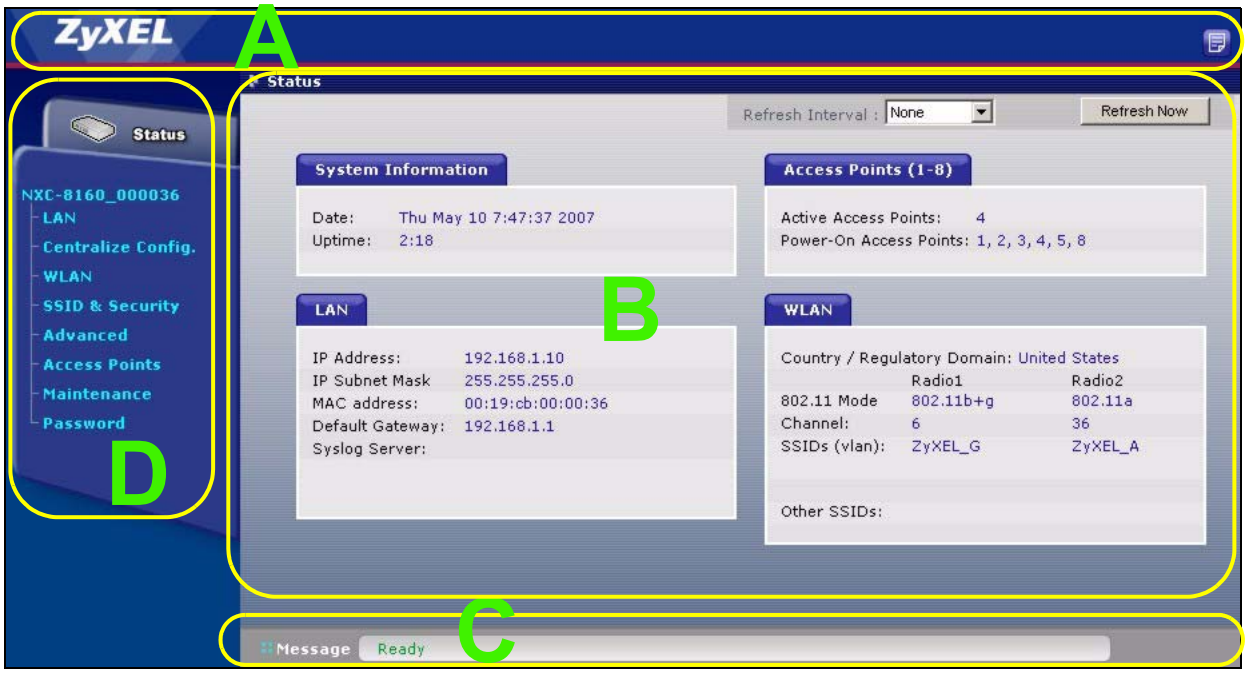
2.2 Accessing the NXC-8160 Web Configurator

1. Make sure your NXC-8160 hardware is properly connected and prepare your computer/ computer network to connect to the NXC-8160 (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type “https://” and the IP address of the switch (for example, the default is 192.168.1.10) in the **Location** or **Address** field. Press **Enter**.
4. The login screen appears. The default username is **admin** and the associated default password is **default**.
5. Click **OK** to view the first web configurator screen.

2.3 Navigating the NXC-8160 Web Configurator

The following summarizes how to navigate the web configurator from the **Status** screen.

Figure 4 Status Screen



As illustrated above, the main screen is divided into these parts:

- **A** - title bar
- **B** - main window
- **C** - status bar
- **D** - navigation panel

2.3.1 Title Bar

The title bar provides a icon in the upper right corner.

The icon provide the following function.

Table 2 Title Bar: Web Configurator Icon

ICON	DESCRIPTION
	**About**: Click this icon to open a screen where you can view the firmware version.

2.3.2 Main Window

The main window shows the screen you select in the navigation panel. It is discussed in more detail in the rest of this document.

Right after you log in, the **Status** screen is displayed.

2.3.3 Status Screen

This screen displays general status information about the NXC-8160.

Figure 5 Web Configurator Status Screen

The following table describes the labels in this screen.

Table 3 Web Configurator Status Screen

LABEL	DESCRIPTION
Refresh Interval	Select a number of seconds or **None** from the drop-down list box to update all screen statistics automatically at the end of every time interval or to not update the screen statistics.
Refresh Now	Click this button to update the status screen statistics immediately.
System Information	
Date	This field displays your NXC-8160's present date and time.
Up Time	This field displays how long the NXC-8160 has been running since it last started up. The NXC-8160 starts up when you turn it on, when you restart it or reset to the defaults (using the **Maintenance** screen).
LAN	
IP Address	This shows the LAN port's IP address.
IP Subnet Mask	This shows the LAN port's subnet mask.
MAC Address	This shows the LAN Ethernet adapter MAC Address of your device.
Default Gateway	This shows the IP address of the gateway in your network.
Syslog Server	This shows the IP address of the server to which the NXC-8160 sends system logs.
Access Points (1-8)	
Active Access Points	This shows the number(s) of the WLAN port(s) to which an active access point is connected.
Power-On Access Points	This shows the number(s) of the WLAN port(s) which is enabled to supply power to an access point.
WLAN	
Country / Regulatory Domain	This shows the country you selected in the **WLAN Configuraion** screen.

Table 3 Web Configurator Status Screen (continued)

LABEL	DESCRIPTION
802.11 Mode	This shows the wireless standard (IEEE 802.11a, b or g) you configured for the radio (wireless transmissions of signals). If **Radio 2** is disabled, this displays **Inactive**.
Channel	This shows the channel number you configured for the radio.
SSIDs (vlan)	This shows the SSID (Service Set IDentity) and the VLAN ID number (if configured) for the radio.
Other SSIDs	This shows the configured SSIDs (if any) which are not assigned to a radio.

2.3.4 Navigation Panel

Use the sub-menus on the navigation panel to configure NXC-8160 features.

The following table describes the sub-menus.

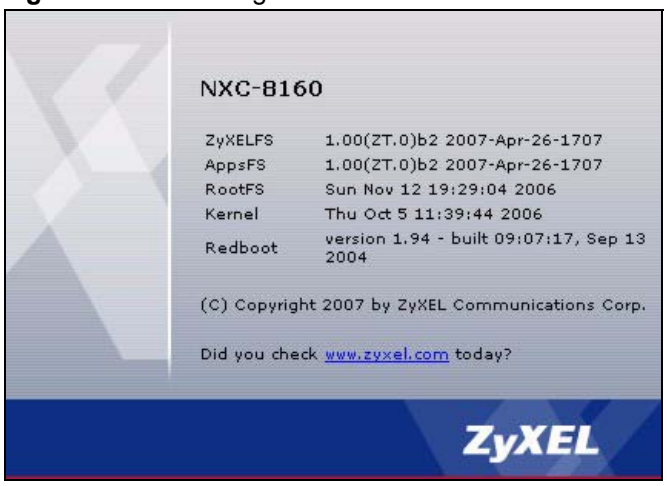
Table 4 Screens Summary

LINK	TAB	FUNCTION
Status		This screen shows the NXC-8160's general device and network status information.
LAN	LAN	Use this screen to configure LAN TCP/IP settings.
WLAN	WLAN Configuration	Use this screen to configure your WLAN settings for a radio and create new SSIDs.
	SSID Table	Use this screen to rename an SSID.
SSID & Security		Use this screen to configure the wireless LAN settings and WLAN security settings for an SSID.
Advanced		Use this screen to set up an alternative NXC-8160 as a backup in case the primary NXC-8160 fails. You can also use this screen to send SNMP traps to an SNMP manager.
Access Points		Use this screen to view which AP is active and decide whether to send power to an AP.
Maintenance	Maintenance	Use this screen to change your NXC-8160's time and date, upload firmware to your NXC-8160, backup and restore the configuration or reset the factory defaults to your NXC-8160. This screen also allows you to reboot the NXC-8160 without turning the power off.
	Syslog & Monitor	Use this screen to enter the IP address of your syslog server and monitor server.
Password		Use this screen to change your system passwords.

2.3.5 About Screen

The **About** screen displays firmware information. To display the screen as shown below, click the about () button.

Figure 6 Web Configurator About Screen



The following table describes the read-only fields in this screen.

Table 5 Web Configurator About Screen

LABEL	DESCRIPTION
ZyXELFS	This field displays the firmware version number and the date created.
AppsFS	This field displays the firmware version number and the date created.
RootFs	This field displays the date and time when RootFs (used as a placeholder inside the firmware kernel) was built.
Kernel	This field displays the date and time when firmware kernel was built.
Redboot	This field displays the Redboot version number and the date created. RedBoot is an embedded system bootstrap and debug firmware from RedHat.

PART II
Web Configurator

3

LAN Screen

This chapter describes how to configure LAN settings.

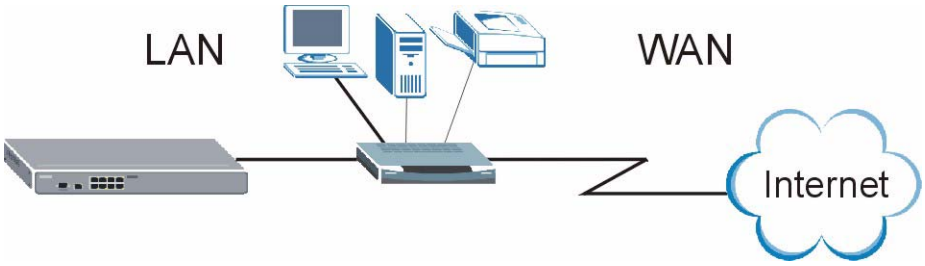
3.1 LAN and WAN

A network is a shared communication system to which many computers are attached.

The Local Area Network (LAN) includes the computers and networking devices (such as the NXC-8160) in your home or office that you connect to a modem or router's LAN ports.

The Wide Area Network (WAN) is another network (most likely the Internet) that you connect to a modem or router. The LAN and the WAN are two separate networks. The following graphic gives an example.

Figure 7 LAN and WAN



3.2 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the connected router. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless

you are told otherwise. If you select 192.168.1.0 as the network number; it covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.10, for your NXC-8160, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your NXC-8160 will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the NXC-8160 unless you are instructed to do otherwise.

3.2.1 Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

3.2.2 Management IP Addresses

The NXC-8160 needs an IP address for it to be managed over the network. The factory default IP address is 192.168.1.10. The subnet mask specifies the network number portion of an IP address. The factory default subnet mask is 255.255.255.0.

3.3 VLAN

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network can belong to more than one group. Only stations within the same group can talk to each other. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s) unless such traffic first goes through a router.

In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain. SSIDs in the same VLAN group share the same broadcast domain thus increase network performance through reduced broadcast traffic.

VLAN on the NXC-8160 allows you to:

- Provide security and isolation among the LAN IP addresses and SSIDs.
- Stop an SSID from accessing the Internet.
- Prevent two SSIDs from communicating with each other or allow specific SSIDs to communicate with each other.
- Improve network performance.
- Provide different services to different VLAN groups by connecting to another VLAN-aware switch.

3.3.1 VLAN Tagging

The NXC-8160 supports IEEE 802.1q VLAN tagging. Tagged VLAN uses an explicit tag (VLAN ID) in the MAC header of a frame to identify VLAN membership. The NXC-8160 can identify VLAN tags for incoming Ethernet frames and add VLAN tags to outgoing Ethernet frames.

When VLAN is enabled, you must connect the NXC-8160 to a VLAN-aware device.

3.3.2 VLAN Application Example

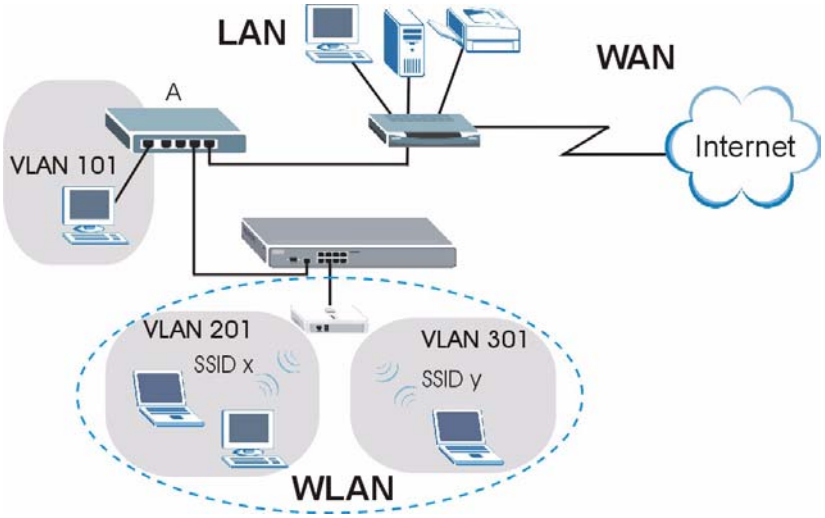
In this example, there is an NXC-8160 and a VLAN-aware switch **A** in your network. The NXC-8160 is connected to port 4 on switch **A**. Port 5 on switch **A** is the uplink port and connected to the Internet. You configure the following VLAN settings on switch **A** and the NXC-8160.

VLAN GROUP	VLAN GROUP MEMBER	
	SWITCH A	NXC-8160
VLAN 101	Port 1, 4	LAN IP Address

VLAN 201	Port 2, 4, 5	SSID x
VLAN 301	Port 3, 4, 5	SSID y

This way, the device connected to port 1 on switch **A** can configure the NXC-8160. Wireless clients connected to SSID **x** or **y** cannot manage the NXC-8160 itself, but they can communicate with port 2 or 3 on switch **A** and access the Internet. Wireless clients connected to SSID **x** cannot talk to wireless clients connected to SSID **y**.

Figure 8 VLAN Application Example

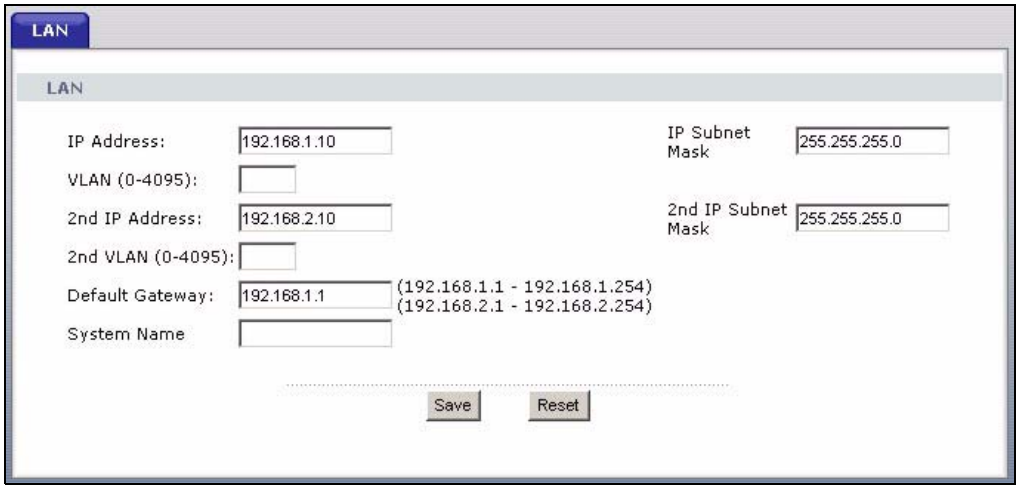


If no devices are in the same VLAN as the NXC-8160 LAN IP address, then you will not be able to configure the NXC-8160 through the LAN port.

3.4 LAN

Click **LAN** to open the **LAN** screen. Use this screen to configure the NXC-8160's IP address and other LAN TCP/IP settings.

Figure 9 LAN



The following table describes the labels in this screen.

Table 6 LAN

LABEL	DESCRIPTION
LAN	You can pre-configure two LAN IP addresses, but only one is in use at a time. 192.168.1.10 is the default IP address.
IP Address	Type the IP address of your NXC-8160 in dotted decimal notation.
IP Subnet Mask	Enter the subnet mask that specifies the network number portion of an IP address.
VLAN (0-4095)	Enter the VLAN identification number (between 0 and 4095) for the LAN IP address. Otherwise, leave this field blank. The LAN IP address's VLAN ID should be unique and cannot be in the same VLAN group as an SSID. That means if you enable VLAN, wireless clients (connected to an SSID on the NXC-8160) cannot communicate with the LAN IP address to configure the NXC-8160. With VLAN, an SSID can still access the Internet through the NXC-8160. Note: All centralized configuration members and the master NXC-8160 should belong to the same VLAN group.
2nd IP Address	Enter a second IP address as the NXC-8160's backup IP address. It should be in a different subnet from the primary one.
2nd IP Subnet Mask	Enter the subnet mask that specifies the network number portion of the second IP address.
2nd VLAN (0-4095)	Enter the VLAN ID of the second IP address. Otherwise, leave this field blank.
Default Gateway	Enter the IP address of the gateway.
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Apply	Click **Apply** to save your changes back to the NXC-8160.
Reset	Click **Reset** to begin configuring this screen afresh.

4

Centralized Configuration

This chapter describes centralized configuration.

4.1 Introduction to Centralized Configuration

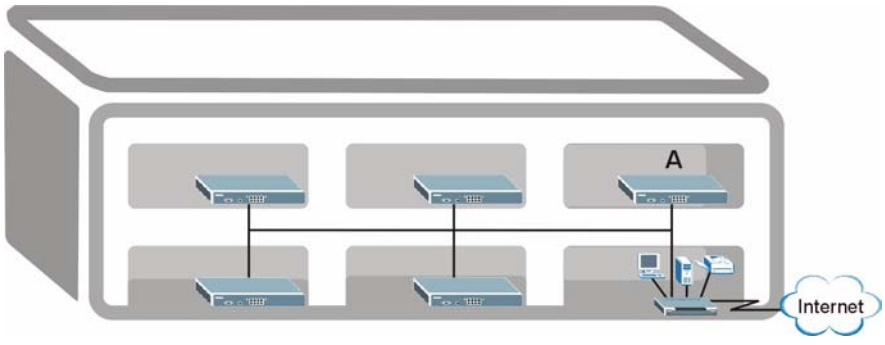
Centralized configuration allows you to configure multiple WLAN controllers through one controller, called the master controller. The controllers must be able to communicate with one another.

Table 7 ZyXEL Centralized Configuration Specifications

Maximum number of centralized configuration members	6
Centralized configuration Member Models	Must be compatible with ZyXEL centralized configuration implementation.
Master Controller	The device through which you manage the member devices.
Member Controllers	The devices being managed by the master device.

In the following example, controller **A** is the master and the other controllers are members.

Figure 10 Centralized Configuration Example



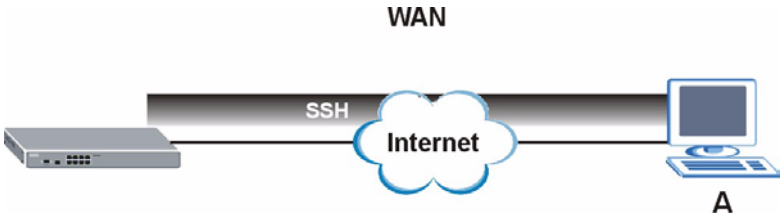
4.2 SSH

You can use SSH (Secure SHell) to securely access the NXC-8160.

Unlike Telnet or FTP, which transmit data in plaintext (clear or unencrypted text), SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. In the following figure, computer **A** on the Internet uses SSH to securely connect to the NXC-8160 for a management session.

If the NXC-8160 is behind a NAT router or a firewall, you need to configure the router or firewall to allow a SSH connection to the NXC-8160.

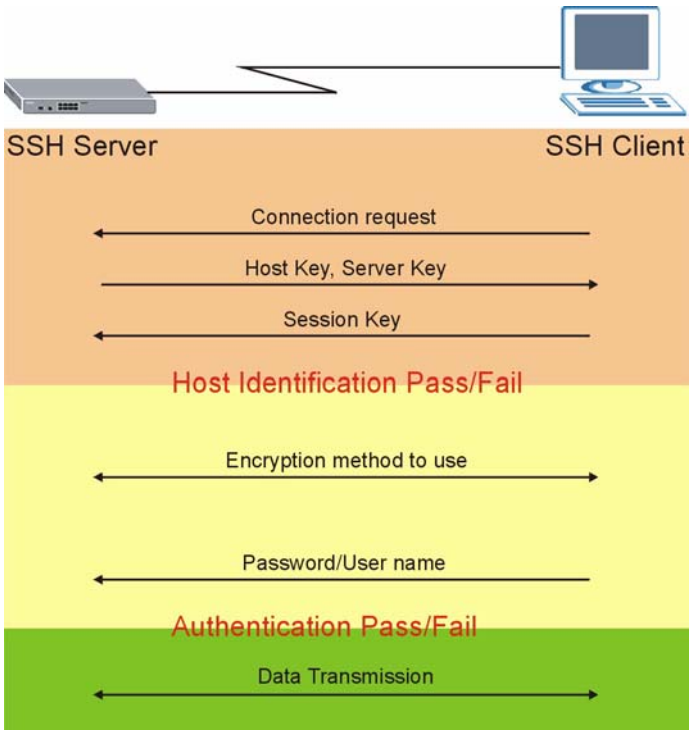
Figure 11 SSH Communication Over the WAN Example



4.3 How SSH Works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 12 How SSH Works



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

4.4 SSH Implementation on the NXC-8160

Your NXC-8160 supports SSH version 1 and 2 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the NXC-8160 for management and file transfer on port 22.

4.4.1 Requirements for Using SSH

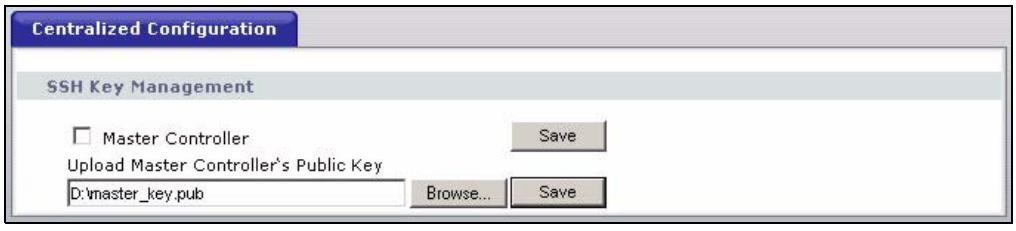
You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the NXC-8160 over SSH.

4.5 Centralized Configuration Screen

Click **Centralized Configuration** to display the screen as shown next. Use this screen to set each NXC-8160 as a master or member controller. The screen changes depending on whether you select the **Master Controller** check box.

By default, the **Master Controller** check box is not selected and the NXC-8160 acts as a member controller.

Figure 13 Centralized Configuration (Member)



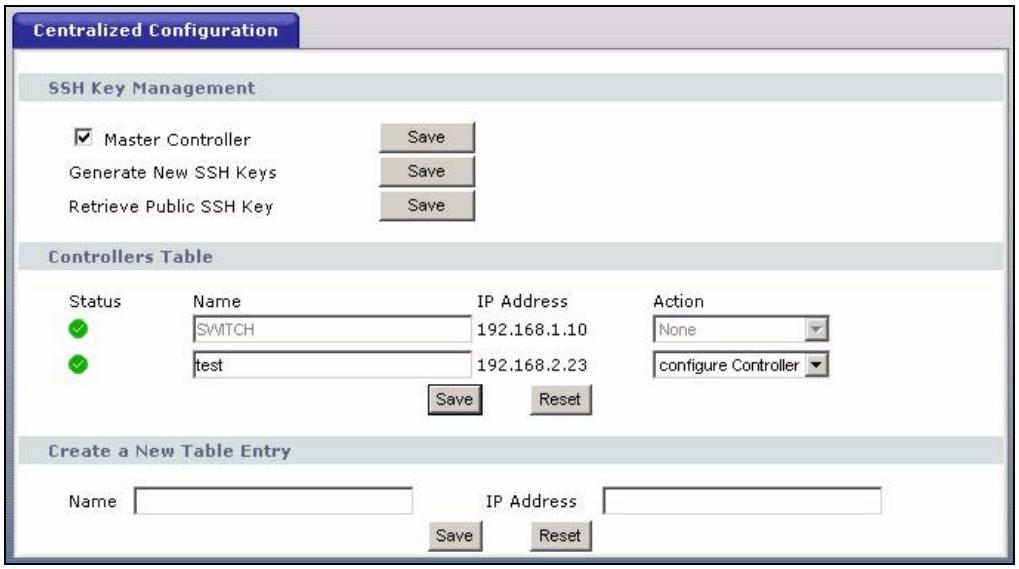
The following table describes the labels in this screen.

Table 8 Centralized Configuration (Member)

LABEL	DESCRIPTION
Master Controller	Clear the check box to have the NXC-8160 act as a member. You can manage the member controllers through the master controller.
Save	Click **Save** to save your customized settings in this section.
Upload Master Controller's Public Key	Click the **Apply** button next to **Upload Master Controller's Public Key** to upload the public key to the NXC-8160. You should have got the key from the main controller and saved it on your computer. See Table 9 on page 44 for more information.
Browse...	Type in the location of the file you want to upload in the field next to **Browse...** or click **Browse...** to find it.
Sve	Click **Save** to save your customized settings. You should go to the **Maintenance** screen and click **Apply** to have your changes take effect immediately without a system rebbot.

When you select **Master Controller** and click **Save**, the screen changes and displays as shown next.

Figure 14 Centralized Configuration (Master)



The following table describes the labels in this screen.

Table 9 Centralized Configuration (Master)

LABEL	DESCRIPTION
SSH Key Management	
Master Controller	When you have more than one NXC-8160 in the network, select this to have your NXC-8160 act as the master controller. You can manage the member controllers in the same network through the master controller.
Save	Click **Save** to save your customized settings.

Table 9 Centralized Configuration (Master)

LABEL	DESCRIPTION
Generate New SSH Keys	Click the **Save** button next to **Generate New SSH Keys** to have the NXC-8160 create a SSH key which is to be used to identify the NXC-8160 for SSH connections.
Retrieve Public SSH Key	Click the **Save** button next to **Retrieve Public SSH Key** to download and save a public key on your computer, so that you can upload the key to a member.
Controllers Table	This table shows the controllers added to the centralized configuration group. The master controller's entry is grayed out. You cannot configure it.
Status	This field displays which indicates the member controller is accessible.
Name	This is the name of a controller you added to this group. To change the name, enter a new one, select **edit entry** in the **Action** field and then click **Save**.
IP Address	This shows the IP address of a controller you added to this group using the fields below.
Action	Select the action that you want to take on the specified member controller. Select **None** to not apply changes to the selected controller. Select **configure controller** to apply this NXC-8160's configuration to the selected controller. Select **reboot controller** to restart the controller. Select **edit entry** to configure the controller's decriptive name. Select **delete entry** to remove the controller from this group.
Save	Click **Save** to save your customized settings in the **Controllers Table** section.
Reset	Click **Reset** to reload the previous configuration for the **Controllers Table** section.
Create a New Table Entry	Use the fields below to add a controller to the centralized configuration group.
Name	Enter the name of the member controller.
IP Address	Enter the IP address of the member controller.
Save	Click **Save** to add a member and display it in the **Controllers Table**.
Reset	Click **Reset** to clear your configuration in the **Create a New Table Entry** section.

5

Wireless LAN

This chapter discusses how to configure wireless LAN on the NXC-8160.

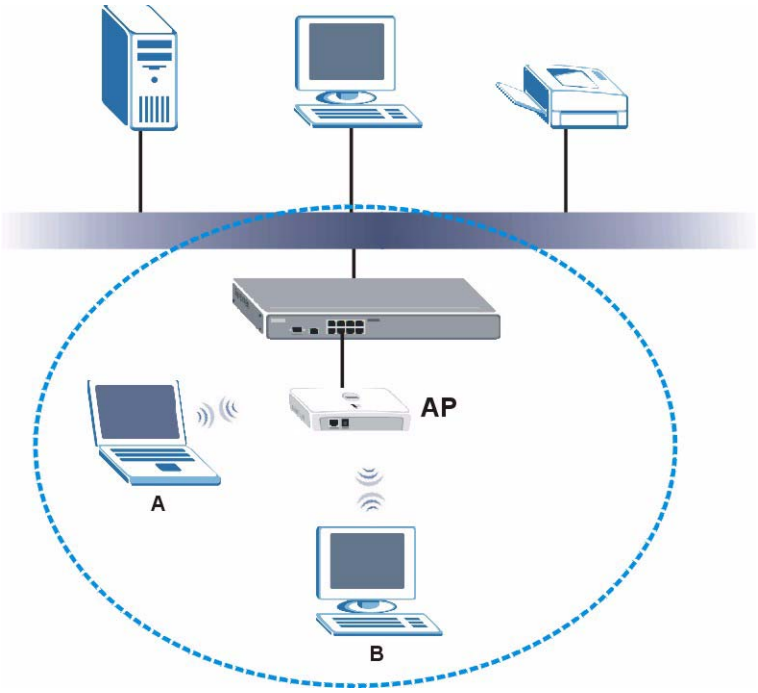
5.1 Wireless LAN Introduction

A wireless LAN can be as simple as two computers with wireless LAN adapters communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN adapters communicating through access points which bridge network traffic to the wired LAN.

See the WLAN appendix for more detailed information on WLANs.

The following figure provides an example of a wireless network.

Figure 15 Example of a Wireless Network



In this wireless network, devices **A** and **B** are called wireless clients. The wireless clients use the access point (AP) which is connected to a WLAN controller to interact with other devices (such as the printer) or with the Internet. Your NXC-8160 is the WLAN controller.

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID.
  The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use different channels.
  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every wireless client in the same wireless network must use security compatible with the AP.
  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

5.2 Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

5.2.1 SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

5.2.2 User Authentication

You can make every user log in to the wireless network before they can use it. This is called user authentication. However, every wireless client in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, there are two typical places to store the user names and passwords for each user.

- In the AP or WLAN controller: this feature is called a local user database or a local database.
- In a RADIUS server: this is a server used in businesses more than in homes.

If your AP or WLAN controller does not provide a local user database and if you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

Local user databases also have an additional limitation that is explained in the next section.

5.2.3 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of user authentication. (See Section 5.2.2 on page 48 for information about this.)

Table 10 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	
↕	WEP	
		WEP + 802.1x (LEAP)
Strongest	WPA-PSK	WPA

For example, if the wireless network has a RADIUS server, you can choose **WEP + 802.1x (LEAP)** or **WPA**. If users do not log in to the wireless network, you can choose no encryption, **WEP** or **WPA-PSK**.

Usually, you should set up the strongest encryption that every wireless client in the wireless network supports. For example, suppose the AP does not have a local user database, and you do not have a RADIUS server. Therefore, there is no user authentication. Suppose the wireless network has two wireless clients. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up **WEP** in the wireless network.

It is recommended that wireless clients use **WPA-PSK**, **WPA**, or stronger encryption. IEEE 802.1x and WEP encryption are better than none at all, but it is still possible for unauthorized devices to figure out the original information pretty quickly.

It is not possible to use **WPA-PSK**, **WPA** or stronger encryption with a local user database. In this case, it is better to set up stronger encryption with no authentication than to set up weaker encryption with the local user database.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every wireless client in the wireless network must have the same key.

5.2.4 Additional Installation Requirements for Using 802.1x

- A computer with an IEEE 802.11 compatible wireless LAN card.
- A computer equipped with a web browser (with JavaScript enabled) and/or Telnet.
- A wireless station must be running IEEE 802.1x-compliant software. Currently, this is offered in Windows XP.
- An optional network RADIUS server for remote user authentication and accounting.

5.3 Introduction to RADIUS

The NXC-8160 can use an external RADIUS server to authenticate users. RADIUS is based on a client-sever model that supports authentication and accounting, where access point is the client and the server is the RADIUS server.

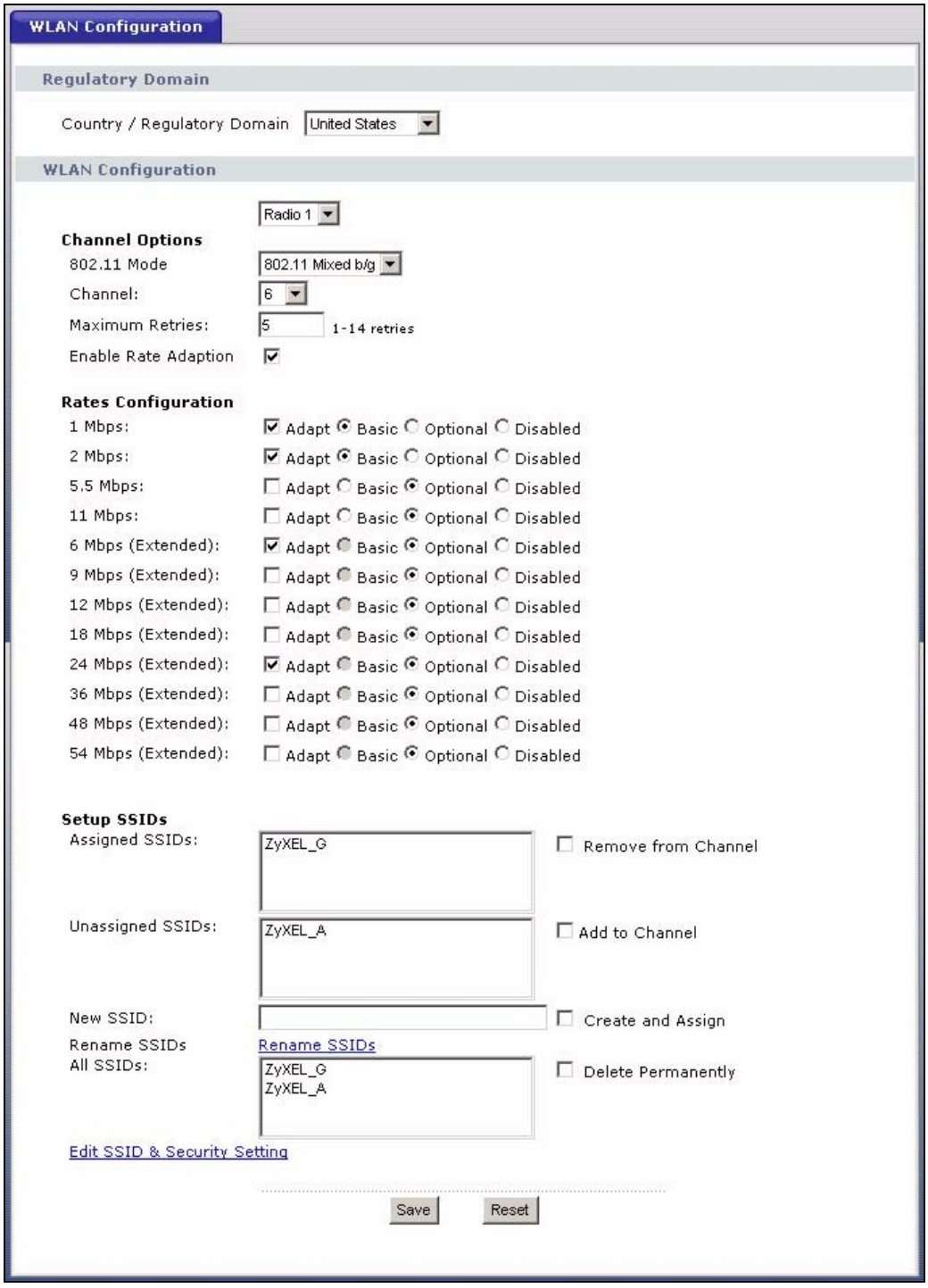
- Authentication
  Determines the identity of the users.
- Accounting
  Keeps track of the client's network activity.

RADIUS user is a simple package exchange in which your NXC-8160 acts as a message relay between the wireless station and the network RADIUS server.

5.4 Configuring WLAN

Click **WLAN** to open the **WLAN Configuration** screen. Use this screen to configure the wireless settings, such as SSID, data rate or channel for each radio.

Figure 16 WLAN



The following table describes the labels in this screen.

Table 11 WLAN

LABEL	DESCRIPTION
Regulatory Domain	
Country/ Regulatory Domain	Select the country where the NXC-8160 is located.
WLAN Configuration	The NXC-8160 supports two radios at the same time. That means you can have two separate wireless networks on the NXC-8160. They can be in the same or different 802.11 mode. Select the radio (**Radio 1**, **Radio 2**) you want to configure in this screen.
Channel Options	
802.11 Mode	Select **802.11a** to allow only IEEE 802.11a compliant WLAN devices to associate with the NXC-8160. Select **802.11b** to allow only IEEE 802.11b compliant WLAN devices to associate with the NXC-8160. Select **802.11g** to allow only IEEE 802.11g compliant WLAN devices to associate with the NXC-8160. Select **802.11 Mixed b/g** to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the NXC-8160. The transmission rate of your NXC-8160 might be reduced. Select **Inactive** to disable **Radio 2**.
Channel	Set the operating frequency/channel depending on your particular region. The options vary depending on the 802.11 mode you selected and the country you are in. Note: The same channel cannot be assigned to both radios.
Maximum Retries	Enter a number (from one to 15) to specify how many times the NXC-8160 tries to send a packet when the transmission fails.
Enable Rate Adaption	Select the check box to have the NXC-8160 operate at the best possible transmission (data) rate. The NXC-8160 can switch between the data rates with the **Adapt** check box selected. When the communication quality drops below a certain level, the NXC-8160 automatically switches to a lower transmission (data) rate. Transmission at lower data speeds is usually more reliable. However, when the communication quality improves again, the NXC-8160 gradually increases the transmission (data) rate again until it reaches the highest available transmission rate.
Rates Configuration	

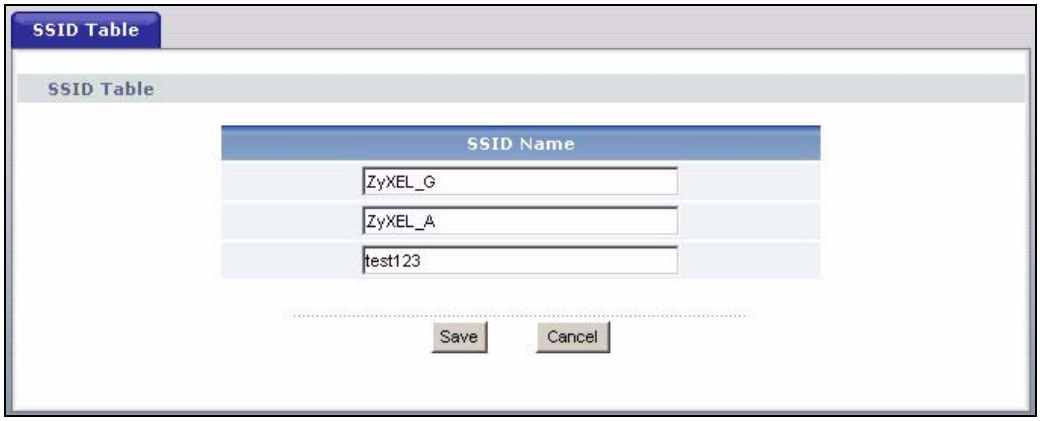
Table 11 WLAN (continued)

LABEL	DESCRIPTION
1 Mbps ~ 54 Mbps	This is the data rate at which the NXC-8160 can transmit. Select **Adapt** to allow the NXC-8160 to switch between and send traffic to wireless clients at the specified rates after you select **Enable Rate Adaption**. If you select **Disabled**, the **Adapt** check box is grayed out and the rate will not be available for rate adaption even if you have selected it. Select **Basic** when your wireless clients can transmit at the specified rate. This allows only the wireless devices that support this data rate or higher to connect to the wireless network. It's recommended that you set the rate supported by all wireless devices in your wireless network as the basic rate. **Basic** is not available for the extended data rates. Select **Optional** to set this rate as an optional choice. The wireless devices that support it can choose to communicate with the network at this rate. Select **Disabled** to not allow the wireless devices to communicate with the network at this rate. You can select **Adapt** and **Basic** or **Optional** at the same time.
Setup SSIDs	The SSID (Service Set IDentifier) identifies the service set with which a wireless client is associated. Wireless clients associating with the access point (AP) must have the same SSID. When a wireless client scans for an AP to associate with, this is the name that is broadcast and seen in the wireless client utility.
Assigned SSIDs	This text box shows the SSID(s) which is assigned to this radio. You can create and assign up to 16 SSIDs to a radio. Select an SSID and click **Remove from Channel** to delete the SSID from this radio after you click **Save**. Note: You cannot delete all SSIDs from a radio.
Unassigned SSIDs	This text box shows the SSID(s) which is created on the NXC-8160 but not assigned to this radio. Select an SSID and click **Add to Channel** to assign it to this radio after you click **Save**. Note: An SSID cannot be assigned to both radios. If you assign the radio an SSID that is already assigned to the other radio, the SSID will be taken out from the other radio.
New SSID	Enter a new SSID and select **Create and Assign** to add this new SSID to this radio after you click **Save**.
Rename SSIDs	Click the **Rename SSIDs** link to open a screen where you can change the SSID(s) created on the NXC-8160. See Section 5.4.1 on page 53 for more information.
All SSIDs	This text box shows all SSIDs available on the NXC-8160. Select an SSID and click **Delete Permanently** to remove it from the NXC-8160.
Edit SSID & Security Setting	Click the link to go to the **SSID & Security** screen where you can configure the wireless and wireless security settings for the specified SSID. See Section 5.5 on page 54 for more information.
Save	Click **Save** to save your changes back to the NXC-8160.
Reset	Click **Reset** to begin configuring this screen afresh.

5.4.1 Rename SSIDs

Click the **Rename SSIDs** link in the **WLAN Configuration** screen to change an existing SSID.

Figure 17 WLAN > SSID Table



The following table describes the labels in this screen.

Table 12 WLAN > SSID Table

LABEL	DESCRIPTION
SSID Name	This displays the SSIDs available on the NXC-8160. Enter a new descriptive name (up to 32 printable English keyboard characters) to replace an existing one.
Save	Click **Save** to save your customized settings.
Cancel	Click **Cancel** to exit this screen without saving.

5.5 Configuring Wireless Security

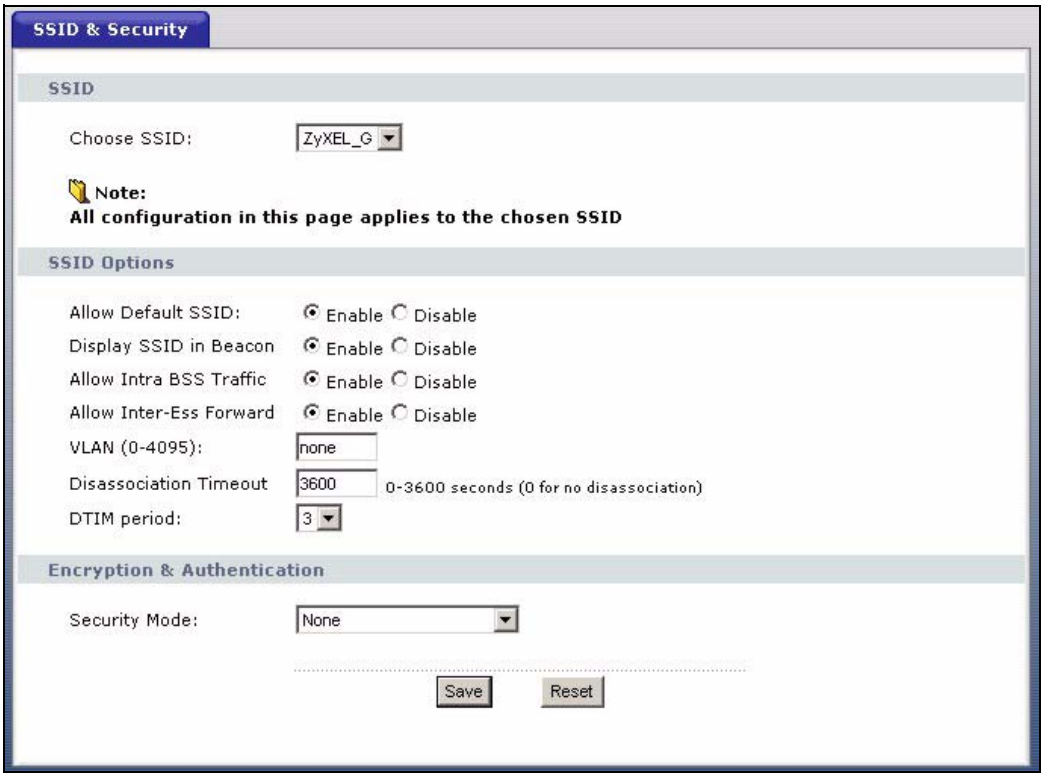
Click **SSID & Security** in the navigation panel or the **SSID & Security** link in the **WLAN Configuration** screen to open the **SSID & Security** screen. Use this screen to onfigure the wireless and wireless security settings for the specified SSID. The screen varies according to the security modes you select.

The following table describes the security modes you can configure.

Table 13 Security Modes

SECURITY MODE	DESCRIPTION
None	Select this to have no data encryption.
WEP64	Select this to use WEP encryption with a static 64bit WEP key.
WEP128	Select this to use WEP encryption with a static 128bit WEP key.
WEP64 & 802.1x (LEAP)	Select this to use 802.1x authentication with a static 64bit WEP key and an authentication server.
WEP128 & 802.1x (LEAP)	Select this to use 802.1x authentication with a static 128bit WEP key and an authentication server.
WPA-PSK	Select this to use WPA with a pre-shared key.
WPA	Select this to use WPA with an authentication server.

Figure 18 SSID & Security



The following table describes the labels in this screen.

Table 14 SSID & Security

LABEL	DESCRIPTION
SSID	
Choose SSID	Select an SSID for which you want to configure the wireless and wireless security settings.
SSID Options	
Allow Default SSID	Select **Enable** to allow a wireless client to connect to a service set on the NXC-8160 even when the wireless client is trying to connect to “any” network. Select **Disable** to allow a wireless client to connect to a service set on the NXC-8160 only when the wireless client is trying to connect to a specific SSID.
Display SSID in Beacon	Select **Enable** to allow the AP to broadcasts the SSID in the area and a client can see it from the utility. Select **Disable** to hide the SSID in the outgoing beacon frame so that a client cannot obtain the SSID through scanning using a site survey tool.
Allow Intra BSS Traffic	A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through the AP(s) and use the same SSID. Intra-BSS traffic is traffic between wireless clients in the BSS. If you select **Enable**, wireless clients in the same BSS can access the wired network and communicate with each other. If you select **Disable**, wireless clients in the same BSS can still access the wired network but cannot communicate with each other.

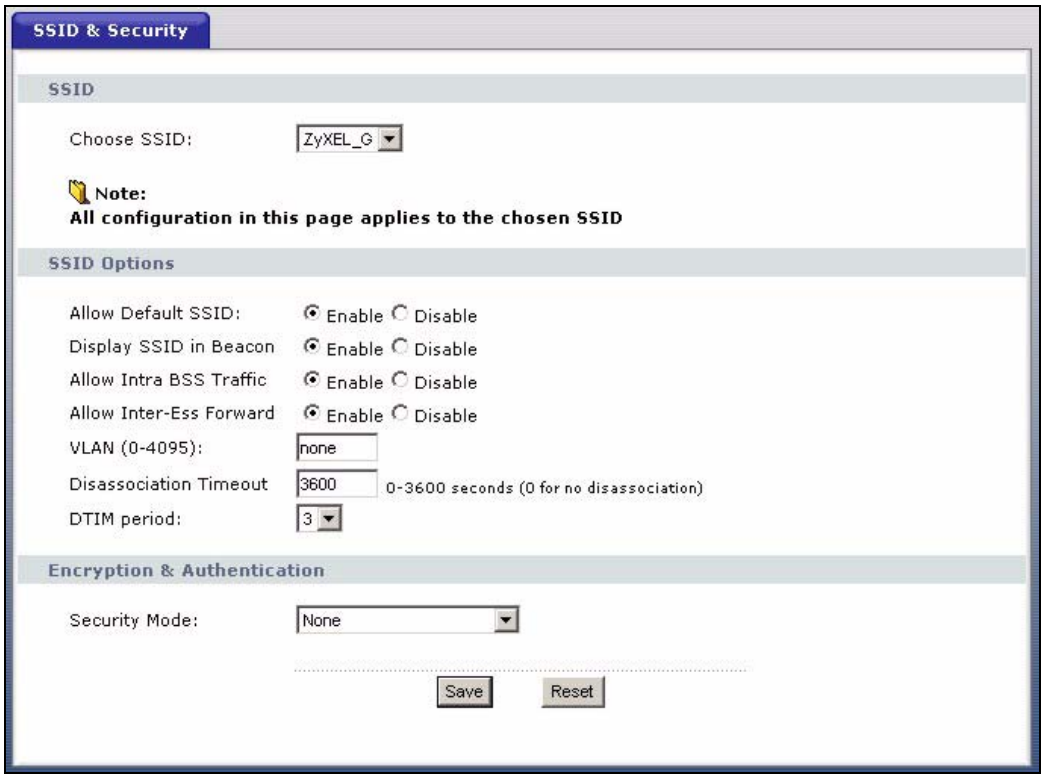
Table 14 SSID & Security (continued)

LABEL	DESCRIPTION
Allow Inter-Ess Forward	An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This type of wireless LAN topology is called an Infrastructure WLAN. Select **Enable** to allow wireless clients using different SSIDs to communicate with each other. Traffic between them will not go through the NXC-8160. Note: To allow Inter-ESS forwarding, you need to enable this feature on both SSIDs. The SSIDs should also belong to the same VLAN group if you activate VLAN. Select **Disable** to stop communications between wireless clients using different SSIDs and all traffic will go through the NXC-8160.
VLAN (0-4095)	A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. Specify a VLAN ID number (between 0 and 4095) to have the SSID belong to one VLAN group. Otherwise, leave this field at its default (**none**).
Disassociation Timeout	Enter the number of seconds (from 0 to 3600) for the NXC-8160 to wait before it automatically disconnect a wireless client from the wired network when there is no traffic sent to or from the wireless client.
DTIM period	A DTIM (Delivery Traffic Indication Message) is used to tell the wireless clients in power-saving mode that a packet is to be sent to them. Select a DTIM period (from 1 to 5) (in beacon intervals). This indicates how many broadcast and multicast packets can be transmitted to wireless clients between two DTIMs.
Save	Click **Save** to save your changes back to the NXC-8160. Your changes take effect only after you click **Apply** in the **Maintenance** screen.
Reset	Click **Reset** to begin configuring this screen afresh.

5.5.1 No Security

If you do not enable any wireless security on your NXC-8160, your network is accessible to any wireless networking device within range.

Figure 19 SSID & Security: None



The following table describes the wireless LAN security labels in this screen.

Table 15 SSID & Security: None

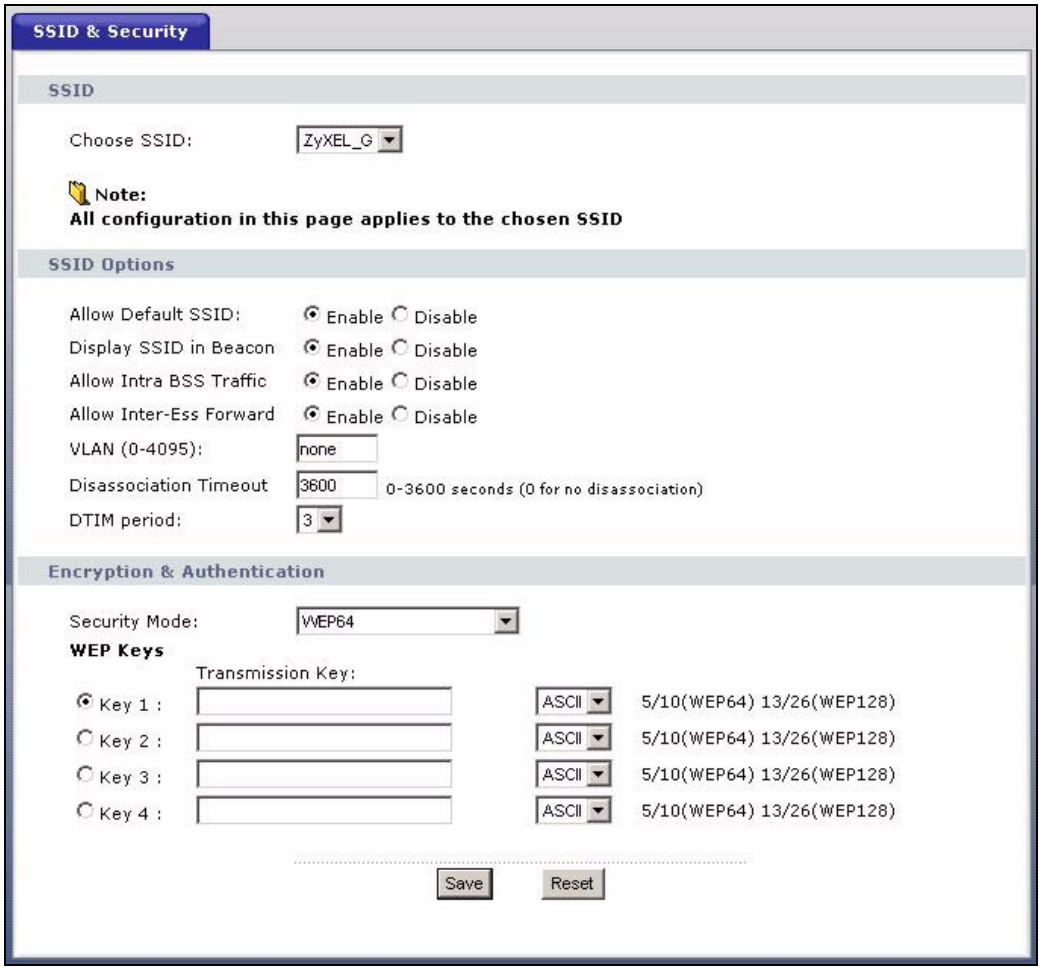
LABEL	DESCRIPTION
Security Mode	Select **None** to allow wireless clients to communicate with the access points without any data encryption.

5.5.2 Static WEP

Static WEP provides a mechanism for encrypting data using encryption keys. Both the AP and the wireless clients must use the same WEP key to encrypt and decrypt data.

Your NXC-8160 allows you to configure up to four 64-bit or 128-bit WEP keys, but only one key can be used at any one time.

Figure 20 SSID & Security: WEP



The following table describes the labels in this screen.

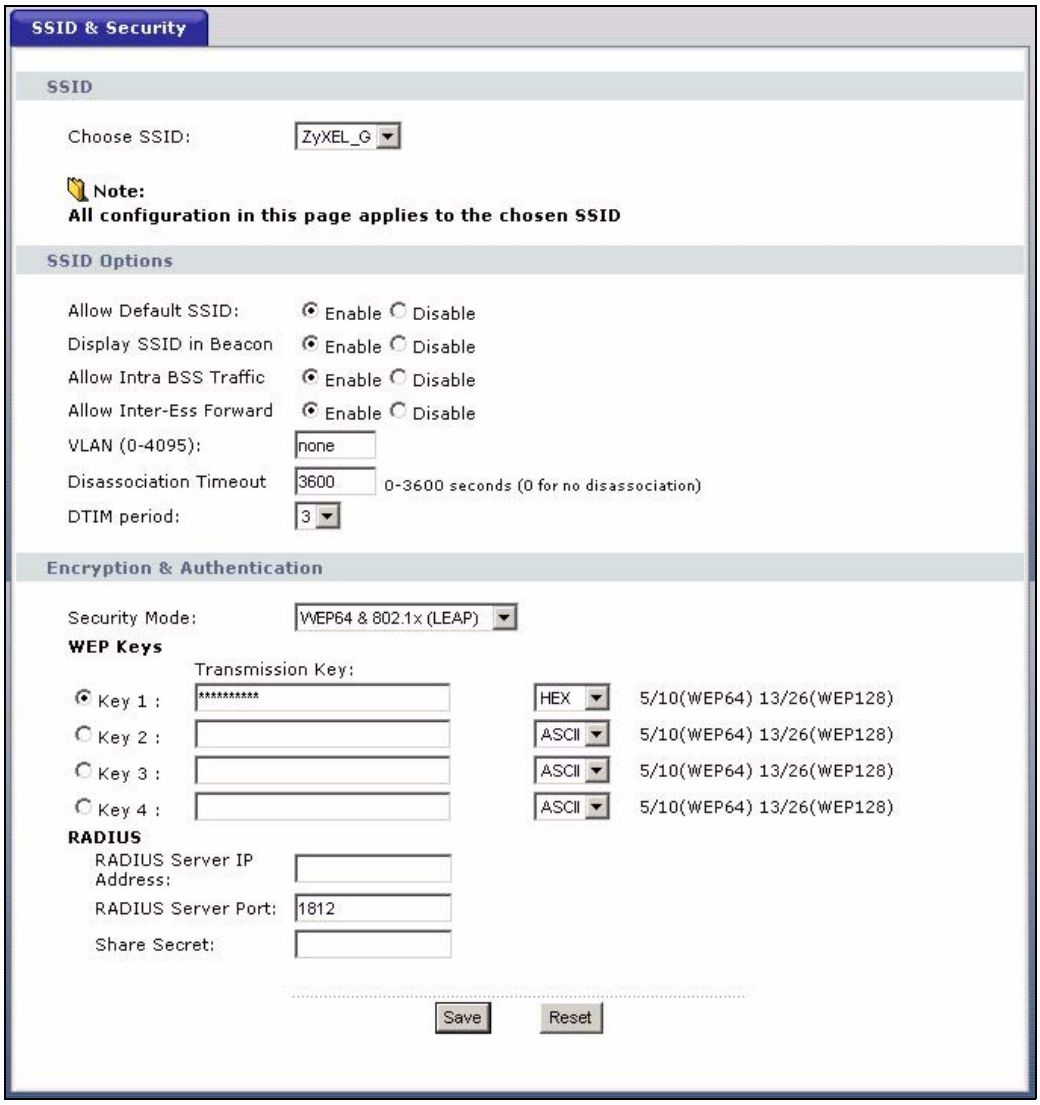
Table 16 SSID & Security: WEP

LABEL	DESCRIPTION
Security Mode	Select **WEP64** or **WEP128** from the drop-down list.
WEP Keys	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network.
Transmission Keys	The WEP keys are used to encrypt data. Both the NXC-8160 and the wireless clients must use the same WEP key for data transmission. You can configure up to four keys, but only one key can be activated at any one time. Select a WEP key to use for data encryption. The default key is key 1. To set the WEP keys, select **ASCII** or **HEX** as the WEP key input method and enter the WEP key in the field provided. Select **ASCII** option to enter ASCII characters as the WEP keys. Select the **HEX** option to enter hexadecimal characters as the WEP keys. If you chose **WEP64** in the **Security Mode** field, then enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each key. If you chose **WEP128** in the **Security Mode** field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each key.

5.5.3 Static WEP + IEEE 802.1x (LEAP)

Select **WEP64 & 802.1x (LEAP)** or **WEP128 & 802.1x (LEAP)** in the **Security Mode** field to display the following screen.

Figure 21 SSID & Security: Static WEP + IEEE 802.1x (LEAP)



The following table describes the labels in this screen.

Table 17 SSID & Security: Static WEP + IEEE 802.1x (LEAP)

LABEL	DESCRIPTION
Security Mode	Select **WEP64 & 802.1x (LEAP)** or **WEP128 & 802.1x (LEAP)** from the drop-down list.
WEP Keys	WEP (Wired Equivalent Privacy) provides data encryption to prevent unauthorized wireless stations from accessing data transmitted over the wireless network.

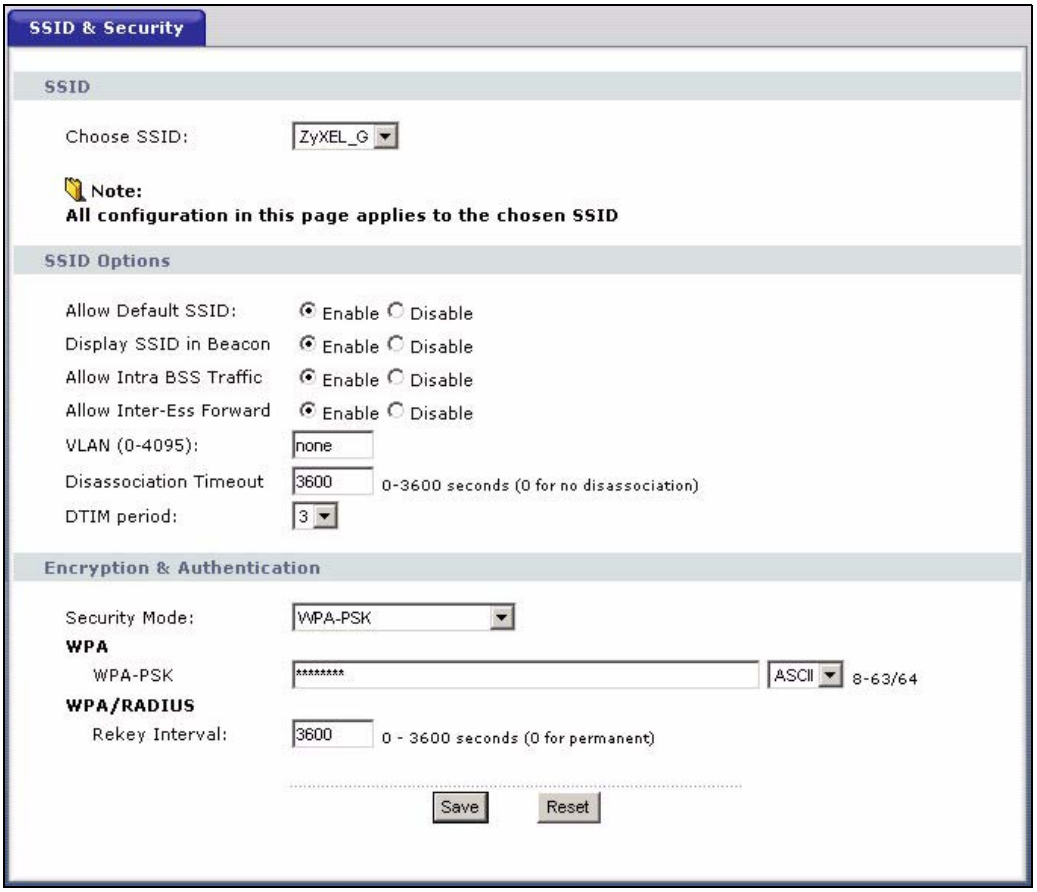
Table 17 SSID & Security: Static WEP + IEEE 802.1x (LEAP) (continued)

LABEL	DESCRIPTION
Transmission Keys	The WEP keys are used to secure your data from eavesdropping by unauthorized wireless users. Both the NXC-8160 and the wireless clients must use the same WEP key for data transmission. You can configure up to four keys, but only one key can be activated at any one time. Select a WEP key to use for data encryption. The default key is key 1. To set the WEP keys, select **ASCII** or **HEX** as the WEP key input method and enter the WEP key in the field provided. Select **ASCII** option to enter ASCII characters as the WEP keys. Select the **HEX** option to enter hexadecimal characters as the WEP keys. If you chose **WEP64** in the **Security Mode** field, then enter 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F") for each key. If you chose **WEP128** in the **Security Mode** field, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F") for each key.
RADIUS	The NXC-8160 can use an external RADIUS server to authenticate users.
RADIUS Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
RADIUS Server Port	The default port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Share Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the NXC-8160. The key is not sent over the network. This key must be the same on the external authentication server and NXC-8160.

5.5.4 WPA-PSK

Select **WPA-PSK** from the **Security Mode** list.

Figure 22 SSID & Security: WPA-PSK



The following table describes the labels in this screen.

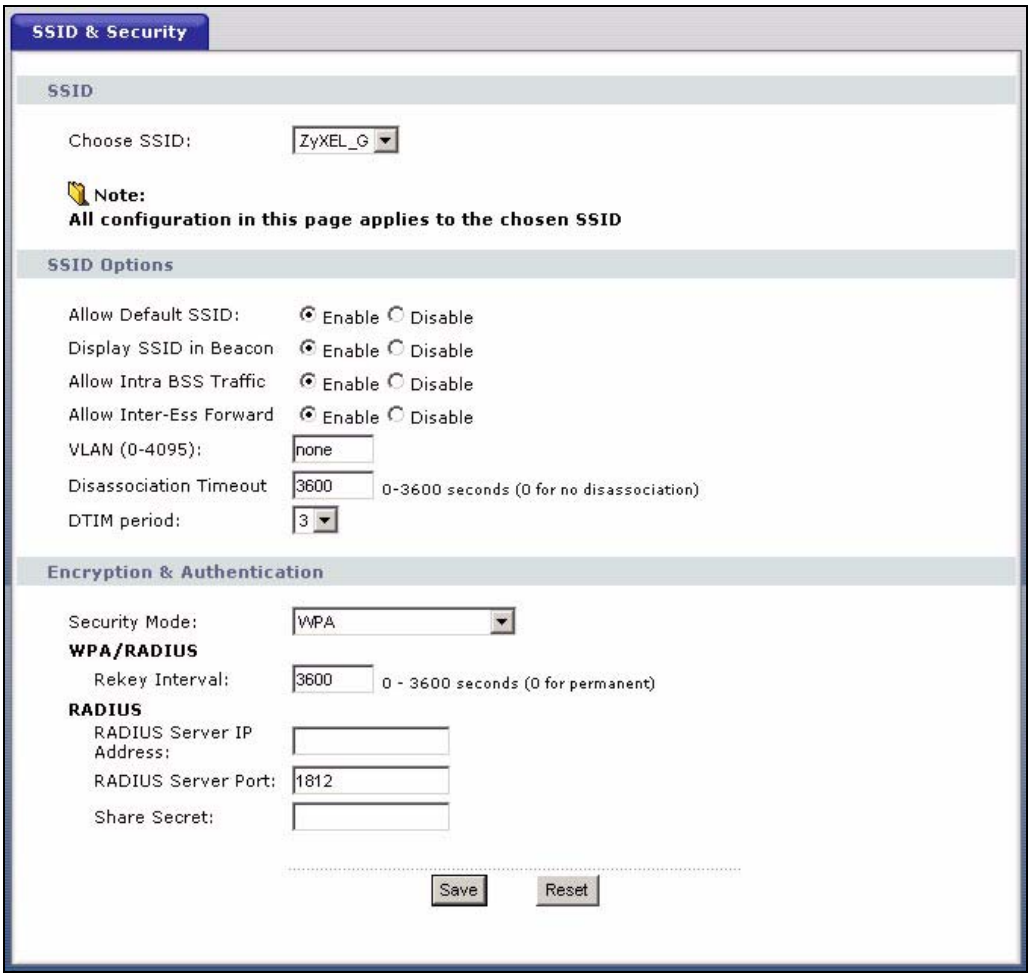
Table 18 SSID & Security: WPA-PSK

LABEL	DESCRIPTION
Security Mode	Select **WPA-PSK** from the drop-down list.
WPA	
WPA-PSK	The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials. Select **ASCII** or **HEX** as the key input method and enter the key in the field provided. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols) or of 64 hexadecimal characters ("0-9", "A-F").
WPA/RADIUS	
Rekey Interval	This is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Enter a time interval between 0 and 3600 seconds.

5.5.5 WPA

Select **WPA** from the **Security Mode** list.

Figure 23 SSID & Security: WPA



The following table describes the labels in this screen.

Table 19 SSID & Security: WPA

LABEL	DESCRIPTION
Security Mode	Select **WPA** from the drop-down list.
WPA/RADIUS	
Rekey Interval	This is the rate at which the RADIUS server sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Enter a time interval between 0 and 3600 seconds.
RADIUS	The NXC-8160 can use an external RADIUS server to authenticate an unlimited number of users.
RADIUS Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
RADIUS Server Port	The default port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so with additional information.
Share Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the NXC-8160. The key is not sent over the network. This key must be the same on the external authentication server and NXC-8160.

6

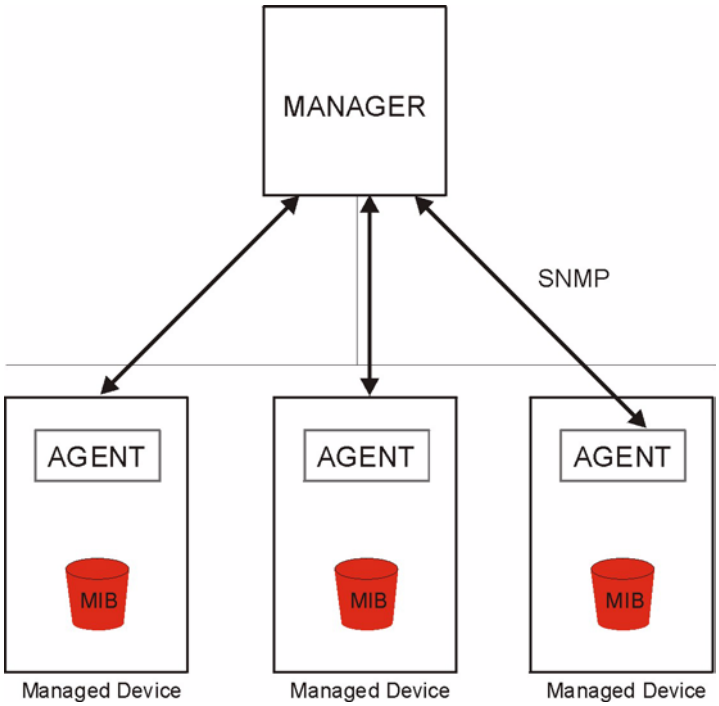
Advanced Screen

This chapter describes how to configure switch redundancy and SNMP settings.

6.1 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your NXC-8160 supports SNMP agent functionality, which allows a manager station to manage and monitor the NXC-8160 through the network. The NXC-8160 supports SNMP version one (SNMPv1). The next figure illustrates an SNMP management operation.

Figure 24 SNMP Management Model



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the NXC-8160). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

6.1.1 SNMP Traps

The NXC-8160 can send the following traps to the SNMP manager.

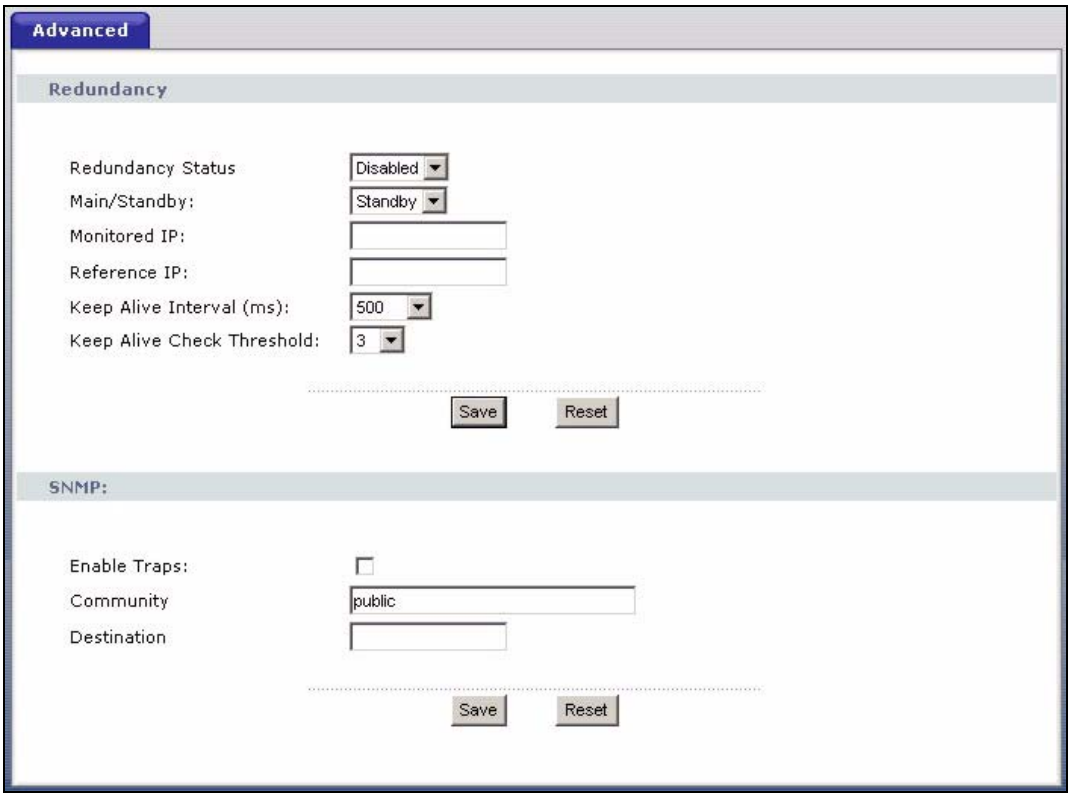
Table 20 SNMP Traps

TRAP NAME	DESCRIPTION
Configured and connected APs of channel [<channel number>]	This trap is sent when an AP is disconnected or connected from/to the WLAN controller.
AP <ap number in hex base> has been connected	This trap is sent when an AP is connected to the WLAN controller.
AP <ap number in hex base> has been disconnected	This trap is sent when an AP is disconnected from the WLAN controller.
Reference Host is up	This trap is sent when the referenced host is up.
Reference Host is down	This trap is sent when the referenced host is down.
Standby Switch is up	This trap is sent when the backup WLAN controller is up.
Standby Switch is down	This trap is sent when the backup WLAN controller is down.
Inactive - Reference Host is down	This trap is sent when the referenced host is down and the main WLAN controller becomes inactive.
Inactive Standby Switch - Main Switch is up	This trap is sent when the backup WLAN controller is deactived because the main WLAN controller becomes active.
Main Switch is active again	This trap is sent when the main WLAN controller becomes active again.
Failure detected in Main Switch - Switching Over	This trap is sent when the main WLAN controller is down and then the backup WLAN controller is enabled.

6.2 Configuring the Advanced Screen

Click **Advanced** to display the screen as shown.

Figure 25 Advanced



The following table describes the labels in this screen.

Table 21 Advanced

LABEL	DESCRIPTION
Redundancy	
Redundancy Status	Select **Enabled** to turn on redundancy between a pair of NXC-8160s. You can deploy one NXC-8160 as the main controller and the other as the backup one. Otherwise, select **Disabled**.
Main/Standby	When you have two NXC-8160s in the network, select **Main** to have this NXC-8160 acts as the active WLAN controller and set another NXC-8160 as the backup WLAN controller. Otherwise, select **Standby** and this NXC-8160 will function as a backup. The backup WLAN controller periodically tests the connections to the main WLAN controller and the referenced host. If the connection to the main WLAN controller is down and the connection to the referenced host is up, the backup WLAN controller becomes active automatically. If the main WLAN controller fails, wireless clients can automatically connect to the backup WLAN controller.
Monitored IP	Enter the IP address of the other WLAN controller.
Reference IP	Eenter the IP address of a reliable nearby computer to have the NXC-8160 ping that address and test the connection to the LAN.
Keep Alive Interval (ms)	The NXC-8160 tests the connection by periodically sending a ping to the address in the **Reference IP** field. Select a number of seconds to set the time interval between checks. Allow more time if your destination IP address handles lots of traffic.
Keep Alive Check Threshold	Select the number of the lost packets that can be allowed before the the connection is considered "down" (not connected).

Table 21 Advanced

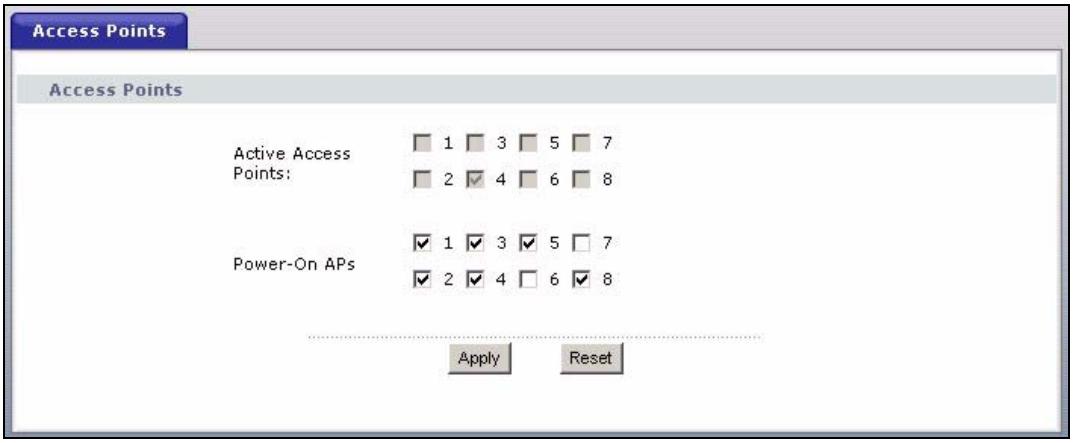
LABEL	DESCRIPTION
Save	Click **Save** to save your customized settings in this section.
Reset	Click **Reset** to begin configuring this section of the screen afresh.
SNMP	
Enable Traps	Select the check box to enable sending of SNMP traps to a station.
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
Save	Click **Save** to save your customized settings in this section.
Reset	Click **Reset** to begin configuring this section of the screen afresh.

7

Access Points Screen

Click **Access Points** to display the screen as shown. This screen allows you to view the status of the access points (APs) connected to the NXC-8160. You can also use this screen to set the NXC-8160 not to supply power to an AP.

Figure 26 Access Points



The following table describes the labels in this screen.

Table 22 Access Points

LABEL	DESCRIPTION
Active Access Points	This field is grayed out and shows whether an access point connected to the WLAN port is active (selected) or not (cleared). By default, an AP receives power from the NXC-8160 and is activated automatically when it is connected to the NXC-8160. The check boxes correspond to the WLAN ports on the front panel of the NXC-8160.
Power-On APs	Select a check box to have the NXC-8160 supply power to the AP connected to this port. Otherwise, clear the check box and the NXC-8160 stops supplying power to the AP connected to this port after you click **Apply**.
Apply	Click **Apply** to save your customized settings.
Reset	Click **Reset** to begin configuring this screen afresh.

8

Maintenance Screen

This chapter displays information on the maintenance screens.

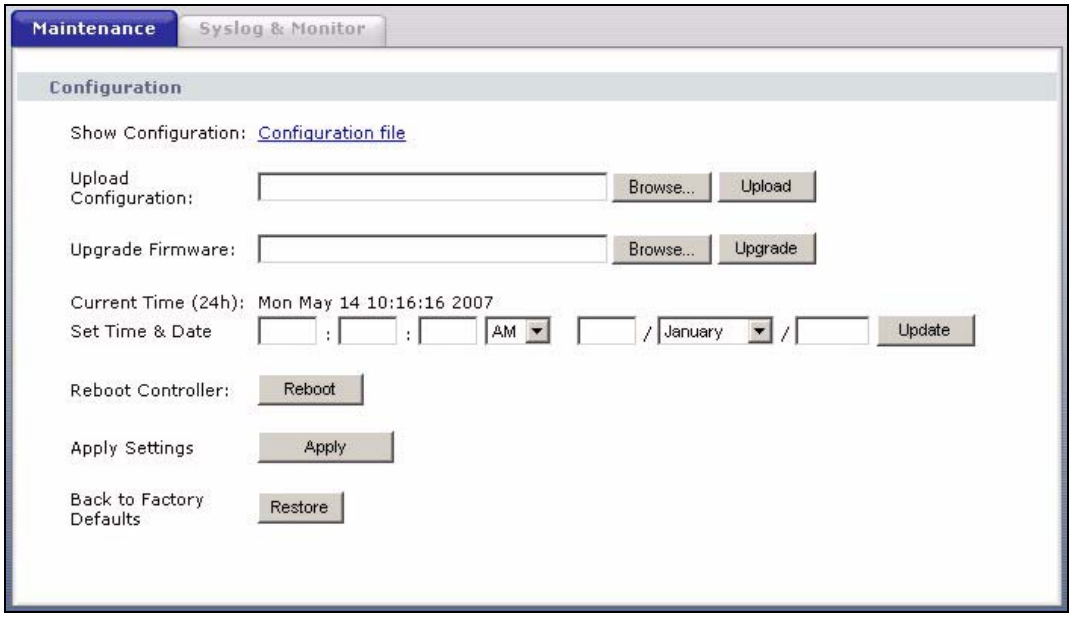
8.1 Maintenance Overview

The maintenance screens can help you view the configuration, upload new firmware, manage configuration, configure the NXC-8160's time and restart your NXC-8160.

Only upload firmware for your specific model!

Do not turn off the NXC-8160 while firmware upload is in progress!

Figure 27 Maintenance



The following table describes the labels in this screen.

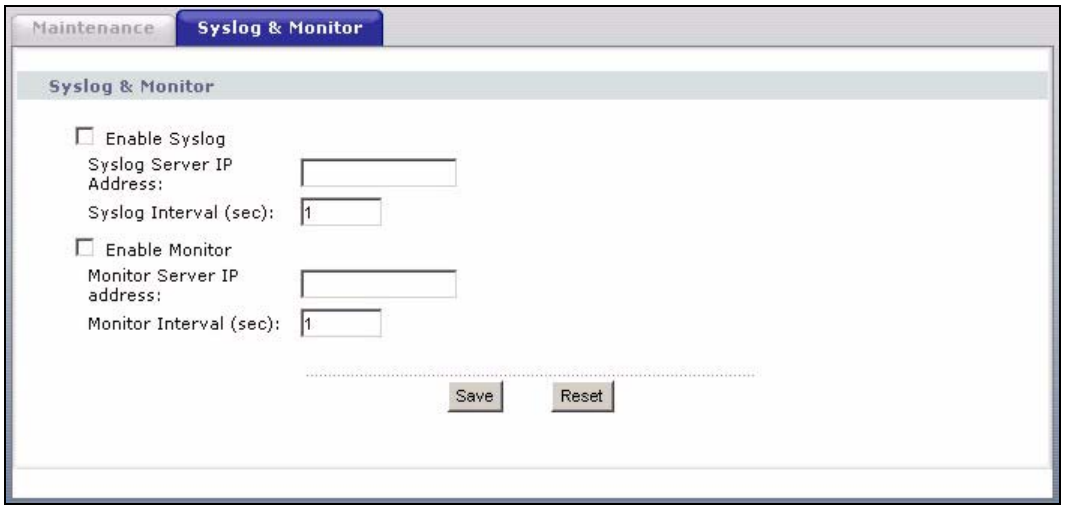
Table 23 Access Points

LABEL	DESCRIPTION
Show Configuration	Click the **Configuration file** link to display the NXC-8160's currect configuration settings. You can right-click the link and select **Save Target As...** to back up your configuration to an XML file on your computer. The backup configuration file will be useful in case you need to return to your previous settings.
Upload Configuration	Load a configuration file from your computer to your NXC-8160. Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click **Upload** to begin the upload process.
Upgrade Firmware	Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "NXC-8160.bin". The upload process uses HTTPs (Hypertext Transfer Protocol over SSL) and may take up to two minutes. After a successful upload, the system will reboot. Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upgrade	Click **Upgrade** to begin the upload process. This process may take up to two minutes.
Current Time (24h)	This field displays the NXC-8160's present time and date
Set Time & Date	Specify the time and date manually. Click **Update** to change the time and date immediately.
Reboot Controller	System restart allows you to reboot the NXC-8160 without turning the power off. Click **Reboot** to restart the NXC-8160 to have your new settings take effect immediately. Restart is different to reset; reset returns the device to its default configuration.
Apply Settings	Not all new changes on the NXC-8160 need a system reboot to take effect. Click **Apply** to apply your changes immediately when a system reboot is not required.
Back to Factory Defaults	Click the **Restore** button to clear all user-entered configuration information and return the NXC-8160 to its factory defaults.

8.2 Configuring Syslog & Monitor

Use this screen to configure to where the NXC-8160 is to send logs and how often a log will be sent. Click **Maintenance** > **Syslog & Monitor**. The screen appears as shown.

Figure 28 Syslog & Monitor



The following table describes the labels in this screen.

Table 24 Syslog & Monitor

LABEL	DESCRIPTION
Enable Syslog	Select the check box to activate syslog logging. Syslog logging sends a system log to an external syslog server.
Syslog Server IP Address	Enter the server name or IP address of the syslog server.
Syslog Interval (sec)	Specify the time interval in seconds (from 1 to 99999) at which the NXC-8160 sends the system logs to the server.
Enable Monitor	Select the check box to send wireless network status logs to an external server.
Monitor Server IP address	Enter the server name or IP address of the monitor server.
Monitor Interval (sec)	Specify the time interval in seconds (from 1 to 99999) at which the NXC-8160 sends the wireless network status logs to the server.
Save	Click **Save** to save your changes back to the NXC-8160.
Reset	Click **Reset** to begin configuring this screen afresh.

9

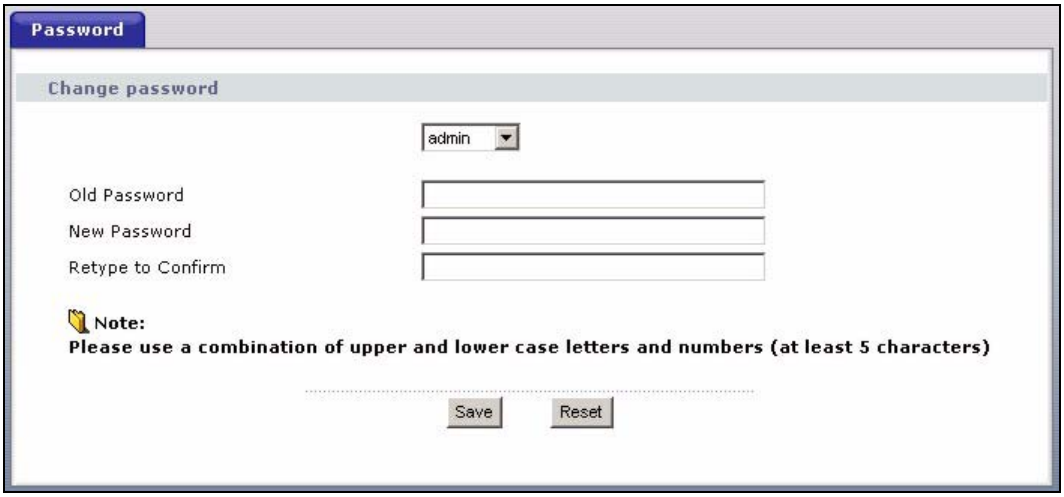
Password

This chapter displays information on the password screen.

9.1 Configuring Password

Click **Password** to open the following screen. Use this screen to change the NXC-8160's management password.

Figure 29 Password



The following table describes the labels in this screen.

Table 25 Password

LABEL	DESCRIPTION
	Select the user name (**admin**, **operator**, or **root**) you want to configure in this screen. To access the web configurator, use the **admin** user name. To configure the NXC-8160 through a secure SSH connection, use the **admin** or **operator** user name. To configure the NXC-8160 via the console port, you can use any one of the user names. The **root** user name has the highest priority. The **admin** user name has the lowest priority. The **root** and **operator** user names can enable debug mode and are for troubleshooting and customer support only.
Old Password	Type the default password or the existing password you use to access the system in this field. By default, the password is **default** for all the user accounts (**admin**, **operator**, or **root**) on the NXC-8160.

Table 25 Password

LABEL	DESCRIPTION
New Password	Type your new system password (at least 5 alphanumeric characters). Note that as you type a password, the screen displays a (*) for each character you type.
Retype to Confirm	Type the new password again for confirmation.
Apply	Click **Save** to save your changes back to the NXC-8160.
Reset	Click **Reset** to begin configuring this screen afresh.

PART III
Troubleshooting and Specifications

10

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- NXC-8160 Access and Login
- Internet Access

10.1 Power, Hardware Connections, and LEDs

The NXC-8160 does not turn on. None of the LEDs turn on.

1. Make sure the NXC-8160 is turned on.
2. Make sure you are using the power cord included with the NXC-8160.
3. Make sure the power cord is connected to the NXC-8160 and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Disconnect and re-connect the power cord to the NXC-8160.
5. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.5 on page 25.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Replace any damaged cables.
4. Disconnect and re-connect the power cord to the NXC-8160.
5. If the problem continues, contact the vendor.

10.2 NXC-8160 Access and Login

I forgot the LAN IP address for the NXC-8160.

1. The default LAN IP address is **192.168.1.10**.
2. If this does not work or you changed the IP address and have forgotten it, you have to contact your vendor.

I forgot the password.

1. The default password is **default**.
2. If this does not work or you changed the password and have forgotten it, you have to contact your vendor.

I cannot see or access the **Login** screen in the web configurator.

1. Make sure you are using the correct IP address.
   - The default LAN IP address is 192.168.1.10 and should begin with “https://”.
   - If you changed the LAN IP address (Section 3.4 on page 38), use the new IP address.
   - If you changed the LAN IP address and have forgotten it, see the troubleshooting suggestions for I forgot the LAN IP address for the NXC-8160.
2. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5 on page 25.
3. Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix C on page 119.
4. Make sure your computer's Ethernet adapter is installed and functioning properly.
5. Make sure your computer is in the same subnet as the NXC-8160. (If you know that there are routers between your computer and the NXC-8160, skip this step.)
   - If there is a DHCP server on your network, make sure your computer is using a dynamic IP address. See Appendix A on page 87.
6. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- You may also need to clear your Internet browser’s cache.

  In Internet Explorer, click **Tools** and then **Internet Options** to open the **Internet Options** screen.

  In the **General** tab, click **Delete** Files. In the pop-up window, select the **Delete all offline content** check box and click **OK**. Click **OK** in the **Internet Options** screen to close it.

- If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer's ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device's MAC address.

  In Windows, use **arp -d** at the command prompt to delete all entries in your computer's ARP table.

I can see the **Login** screen, but I cannot log in to the NXC-8160.

1. Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is **Switch1**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
2. Disconnect and re-connect the power cord to the NXC-8160.
3. If this does not work, you have to contact your vendor.

I cannot Telnet to the NXC-8160.

You cannot use Telnet to access the NXC-8160. The NXC-8160 supports SSH (Secure SHell) and allows a secure encrypted connection for support purposes only.

I cannot access the NXC-8160 or ping any computer from the WLAN.

1. Make sure the wireless adapter on the wireless client is working properly.
2. Make sure the wireless adapter (installed on your computer) is IEEE 802.11 compatible and supports the same wireless standard as the NXC-8160.
3. Make sure your computer (with a wireless adapter installed) is within the transmission range of the AP(s) connected to the NXC-8160.
4. Check that both the NXC-8160 and your wireless client are using the same wireless and wireless security settings.
5. Make sure you didn't enable VLAN on the NXC-8160's LAN IP address and the SSID to which the wireless station is connecting.

10.3 Internet Access

I cannot access the Internet wirelessly through the NXC-8160.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.5 on page 25.
2. Make sure the NXC-8160 is connected to a network that has Internet access.
3. Make sure the wireless and wireless security settings in the wireless client are the same as the settings in the NXC-8160.
4. Make sure the wireless adapter on the wireless client is working properly.
5. Make sure the wireless adapter (installed on your computer) is IEEE 802.11 compatible and supports the same wireless standard as the NXC-8160.
6. Make sure your computer (with a wireless adapter installed) is within the transmission range of the AP(s) connected to the NXC-8160.
7. Make sure the AP(s) connected to the NXC-8160 is receiving power from the NXC-8160 and working properly.

The Internet connection is slow or intermittent.

1. There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.5 on page 25. If the NXC-8160 is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.
2. Check the signal strength. If the signal strength is low, try moving your computer closer to an AP if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).
3. Reboot the NXC-8160 or disconnect and re-connect the power cord to the NXC-8160.
4. If the problem continues, contact the network administrator or vendor.

11

Product Specifications

The following tables summarize the NXC-8160's hardware and firmware features.

Table 26 Hardware Specifications

Dimensions	430 (W) x 240 (D) x 45 (H) mm
Weight	3 Kg
Power Specification	100 - 240 VAC/2A max. Supply 15 W power to each WLAN port
Ethernet Interface	
LAN	One auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet port
WLAN	Eight 100 Mbps RJ-45 Fast Ethernet (IEEE 802.3u) ports which are compliant with the IEEE 802.3af Power over Ethernet standard
Reset Button	Restores factory default settings
Console	RS-232 DB9M
Operation Temperature	0º C ~ 50º C
Storage Temperature	-30º C ~ 60º C
Operation Humidity	10% ~ 95% RH (non-condensing)
Storage Humidity	5% ~ 95% RH (non-condensing)
Certifications	EMC: FCC Part 15 Class B, CE EMC Class B, C-Tick Class B Safety: CSA International, UL60950-1, EN60950-1

Table 27 Firmware Specifications

FEATURE	DESCRIPTION
Default IP Address	192.168.1.10
Default Subnet Mask	255.255.255.0 (24 bits)
Default User Name	admin
Default Password	default
Device Management	Use the web configurator to easily configure the rich range of features on the NXC-8160.
Wireless Functionality	Allow the IEEE 802.11a, IEEE 802.11b and/or IEEE 802.11g wireless clients to connect to the NXC-8160 wirelessly. Enable wireless security (WEP, WPA, WPA-PSK or IEEE 802.1x with static WEP) to protect your wireless network.
Firmware Upgrade	Download new firmware (when available) from the ZyXEL web site and use the web configurator to put it on the NXC-8160. Note: Only upload firmware for your specific model!

Table 27 Firmware Specifications

FEATURE	DESCRIPTION
Configuration Backup & Restoration	Make a copy of the NXC-8160's configuration. You can put it back on the NXC-8160 later if you decide to revert back to an earlier configuration.
IP Multicast	IP multicast is used to send traffic to a specific group of computers. The NXC-8160 supports versions 1 and 2 of IGMP (Internet Group Management Protocol) used to join multicast groups (see RFC 2236).
Time and Date	Get the current time and date from an external server when you turn on your NXC-8160. You can also set the time manually. These dates and times are then used in logs.
Logging and Tracing	Use packet tracing and logs for troubleshooting. You can send logs from the NXC-8160 to an external syslog server.

Cable Pin Assignments

In a serial communications connection, generally a computer is DTE (Data Terminal Equipment) and a modem is DCE (Data Circuit-terminating Equipment). The NXC-8160 is DCE when you connect a computer to the console port.

The pin layout for the DB-9 connector end of the cables is as follows.

Figure 30 Console Cable DB-9 End Pin Layout

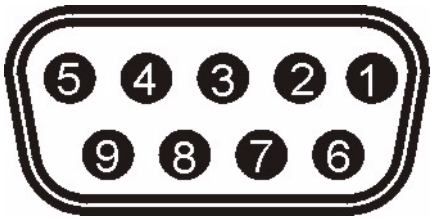


Table 28 Console Port Pin Assignments

CONSOLE Port RS – 232 (Female) DB-9F	DIAL BACKUP RS – 232 (Male) DB-9M
Pin 1 = NON Pin 2 = DCE-TXD Pin 3 = DCE –RXD Pin 4 = DCE –DSR Pin 5 = GND Pin 6 = DCE –DTR Pin 7 = DCE –CTS Pin 8 = DCE –RTS PIN 9 = NON	Pin 1 = NON Pin 2 = DTE-RXD Pin 3 = DTE-TXD Pin 4 = DTE-DTR Pin 5 = GND Pin 6 = DTE-DSR Pin 7 = DTE-RTS Pin 8 = DTE-CTS PIN 9 = NON.

Table 29 Ethernet Cable Pin Assignments

WAN / LAN ETHERNET CABLE PIN LAYOUT			
Straight-through		**Crossover**	
(Switch)	(Adapter)	(Switch)	(Switch)

Table 29 Ethernet Cable Pin Assignments

WAN / LAN ETHERNET CABLE PIN LAYOUT											
1	IRD +		1	OTD +	1	IRD +			1	IRD +
2	IRD -		2	OTD -	2	IRD -			2	IRD -
3	OTD +		3	IRD +	3	OTD +			3	OTD +
6	OTD -		6	IRD -	6	OTD -			6	OTD -

PART IV Appendices and Index

The appendices provide general information. Some details may not apply to your NXC-8160.

A

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP/Vista, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

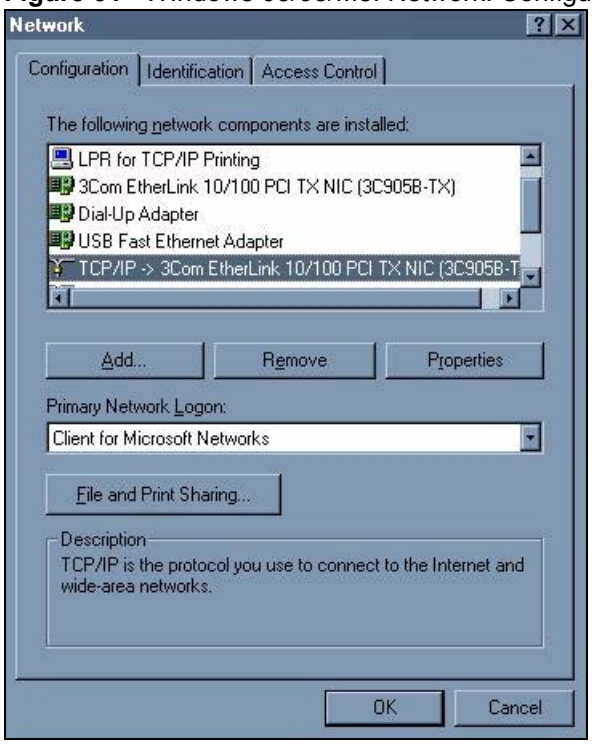
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the NXC-8160's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 31 WIndows 95/98/Me: Network: Configuration



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1. In the **Network** window, click **Add**.
2. Select **Adapter** and then click **Add**.
3. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1. In the **Network** window, click **Add**.
2. Select **Protocol** and then click **Add**.
3. Select **Microsoft** from the list of **manufacturers**.
4. Select **TCP/IP** from the list of network protocols and then click **OK**.

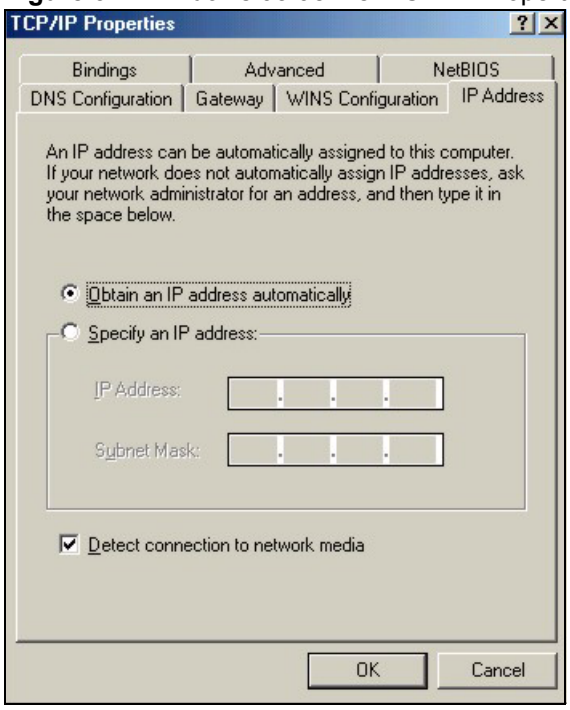
If you need Client for Microsoft Networks:

1. Click **Add**.
2. Select **Client** and then click **Add**.
3. Select **Microsoft** from the list of manufacturers.
4. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
5. Restart your computer so the changes you made take effect.

Configuring

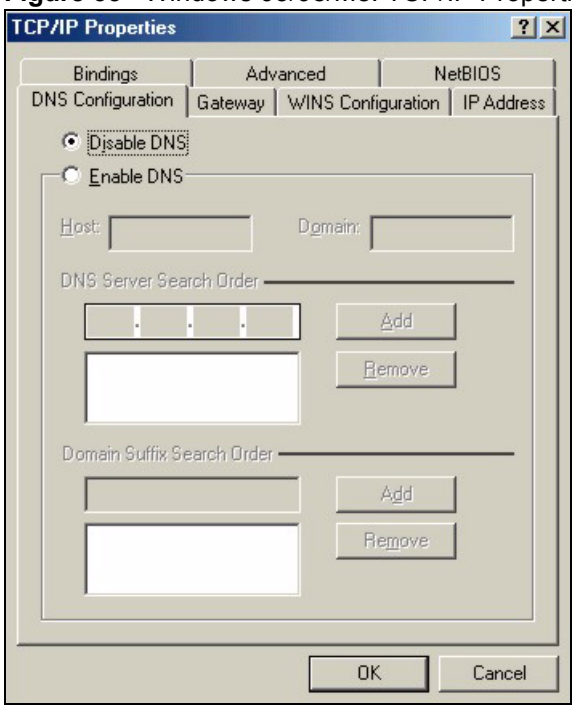
1. In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
2. Click the **IP Address** tab.
   - If your IP address is dynamic, select **Obtain an IP address automatically**.
   - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

Figure 32 Windows 95/98/Me: TCP/IP Properties: IP Address



3. Click the **DNS** Configuration tab.
   - If you do not know your DNS information, select **Disable DNS**.
   - If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 33 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.
   - If you do not know your gateway's IP address, remove previously installed gateways.
   - If you have a gateway IP address, type it in the **New gateway field** and click **Add**.
5 Click **OK** to save and close the **TCP/IP Properties** window.
6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
7 Turn on your NXC-8160 and restart your computer when prompted.

Verifying Settings

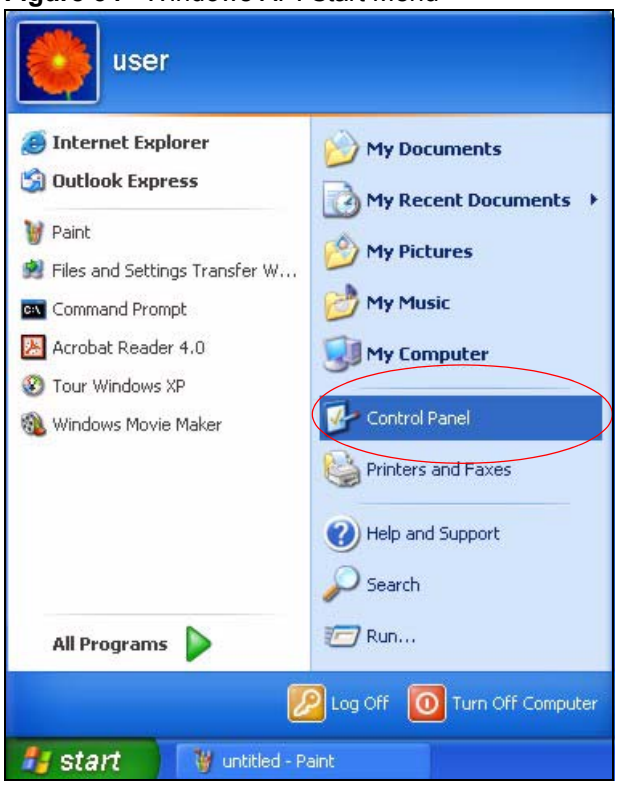
1 Click **Start** and then **Run**.
2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 34 Windows XP: Start Menu

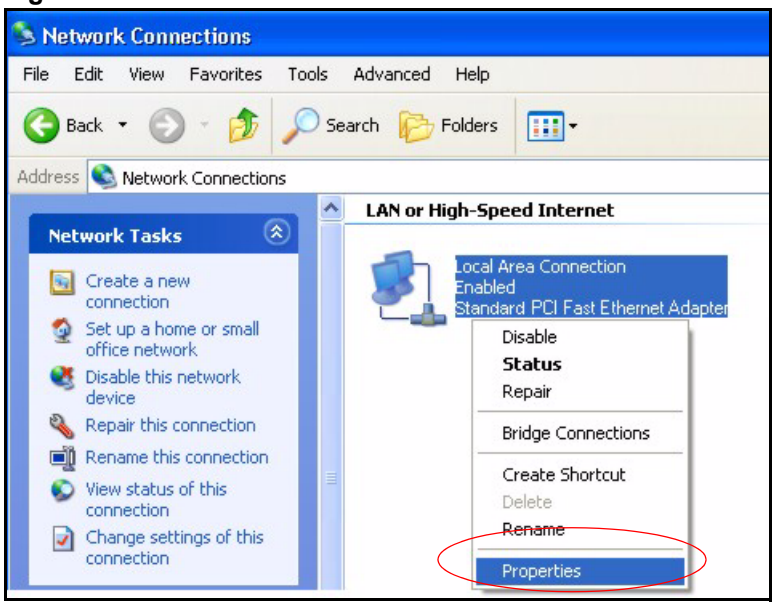


2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 35 Windows XP: Control Panel

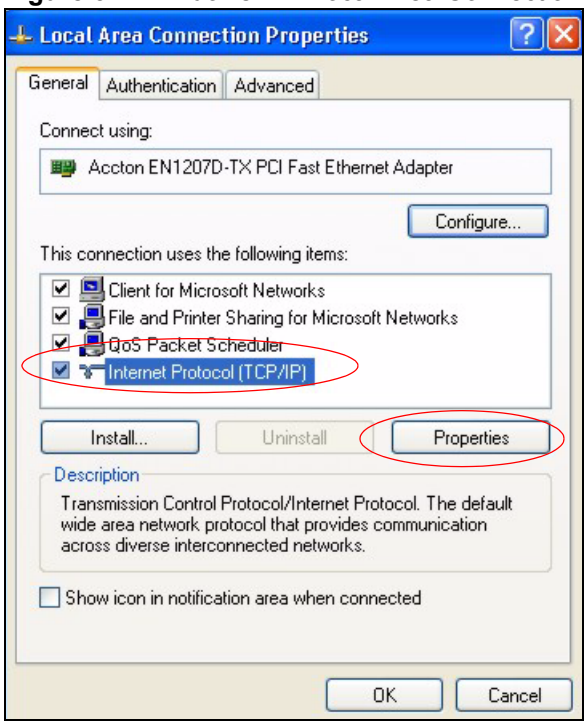
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 36 Windows XP: Control Panel: Network Connections: Properties



4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

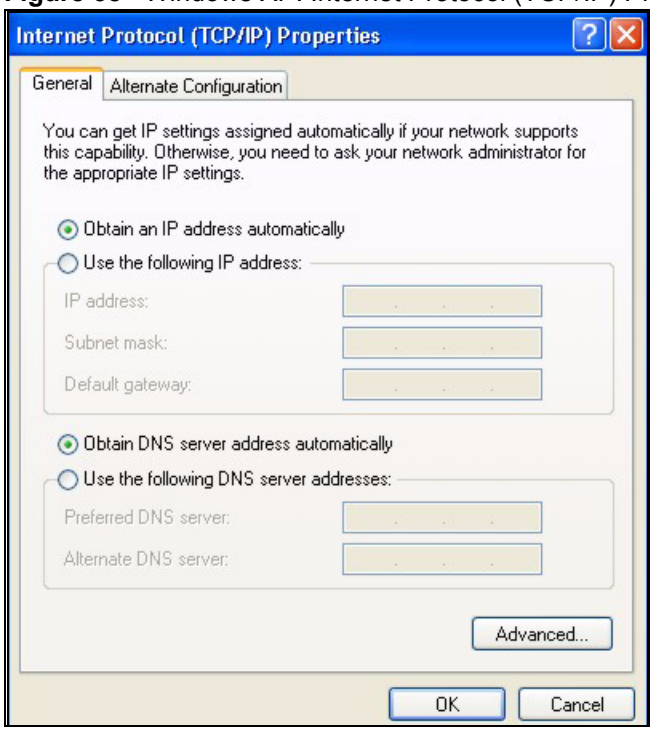
Figure 37 Windows XP: Local Area Connection Properties



5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

Figure 38 Windows XP: Internet Protocol (TCP/IP) Properties

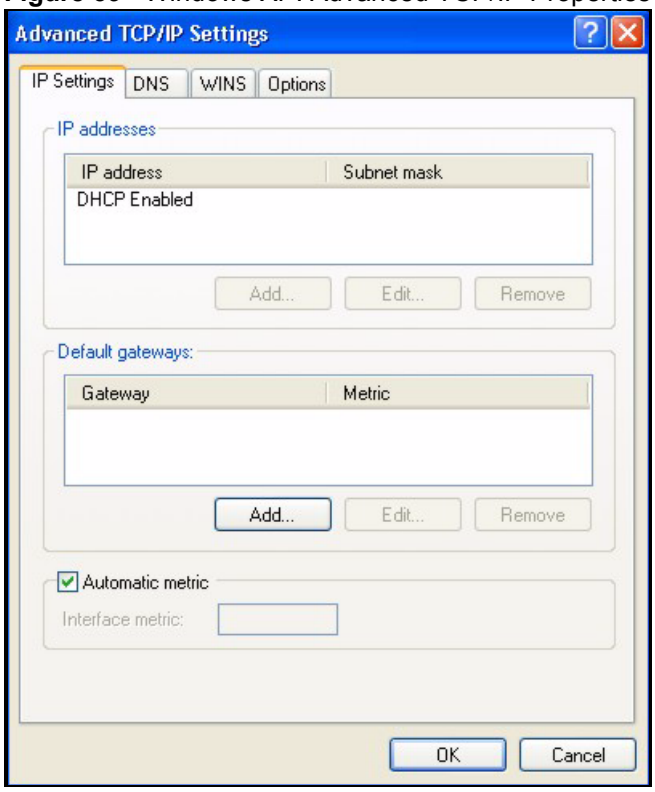


6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 39 Windows XP: Advanced TCP/IP Properties

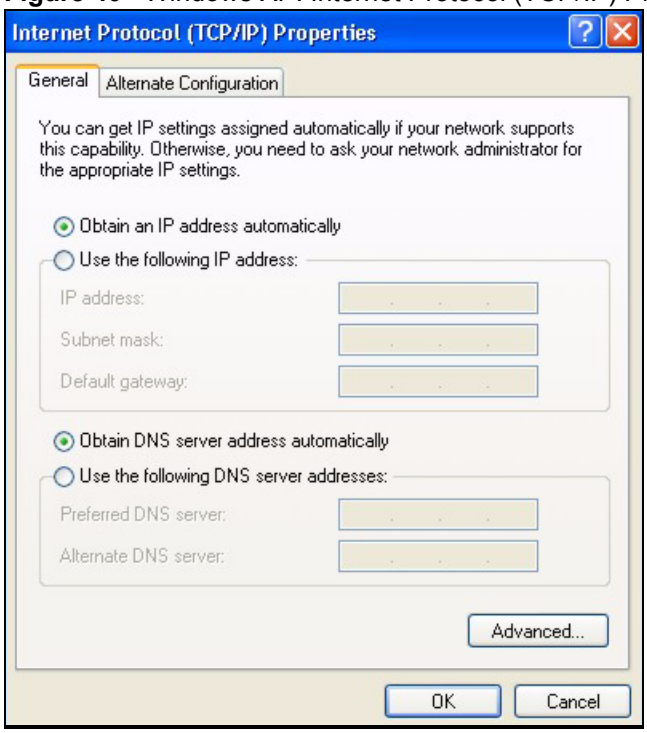


7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 40 Windows XP: Internet Protocol (TCP/IP) Properties



8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 Turn on your NXC-8160 and restart your computer (if prompted).

Verifying Settings

1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

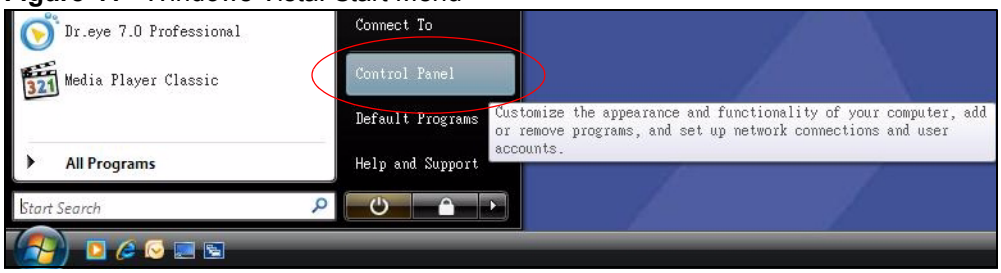
2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Windows Vista

This section shows screens from Windows Vista Enterprise Version 6.0.

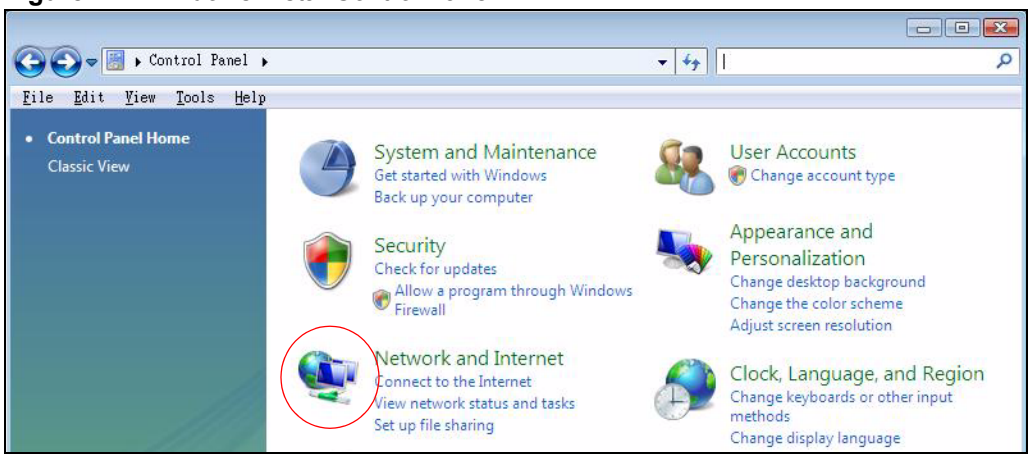
1 Click the **Start** icon, **Control Panel**.

Figure 41 Windows Vista: Start Menu



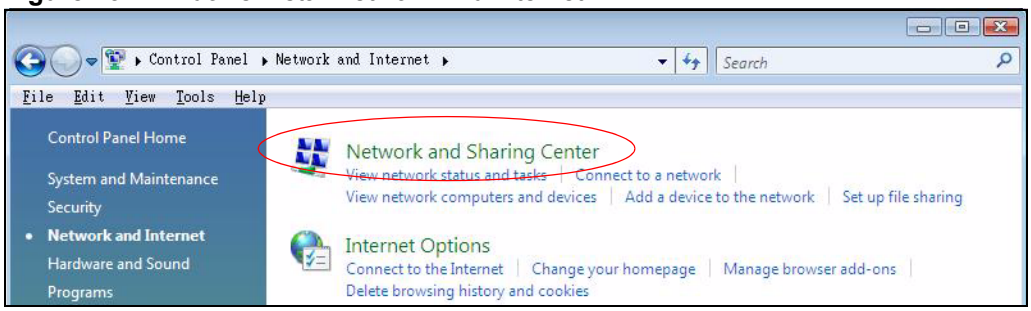
2 In the **Control Panel**, double-click **Network and Internet**.

Figure 42 Windows Vista: Control Panel



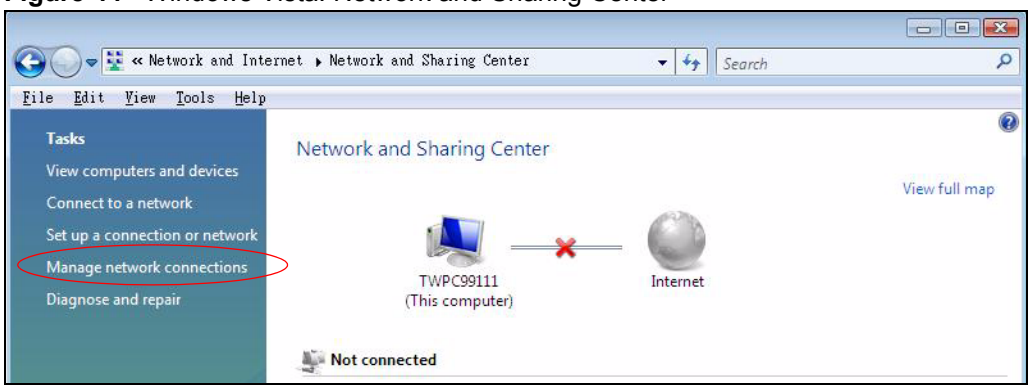
3 Click **Network and Sharing Center**.

Figure 43 Windows Vista: Network And Internet



4 Click **Manage network connections**.

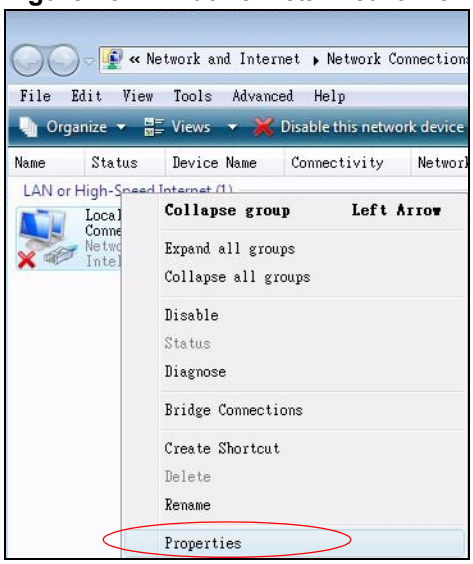
Figure 44 Windows Vista: Network and Sharing Center



5 Right-click **Local Area Connection** and then click **Properties**.

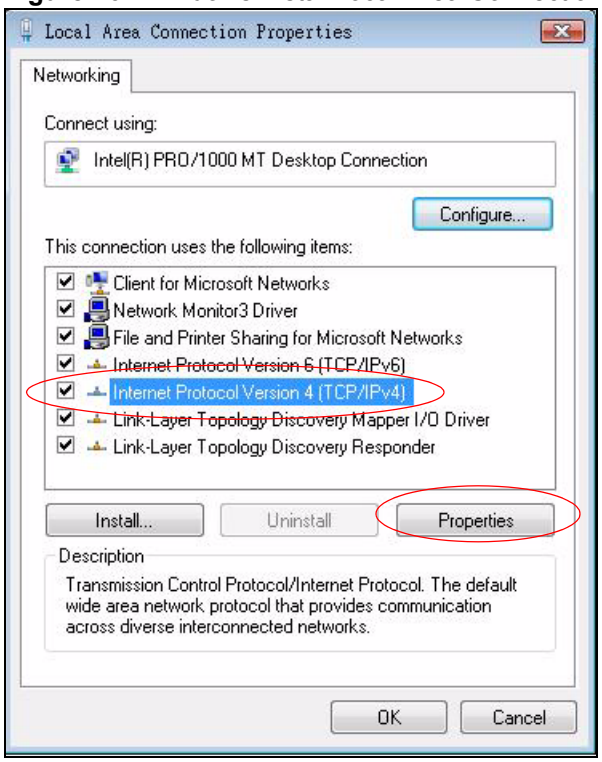
During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

Figure 45 Windows Vista: Network and Sharing Center



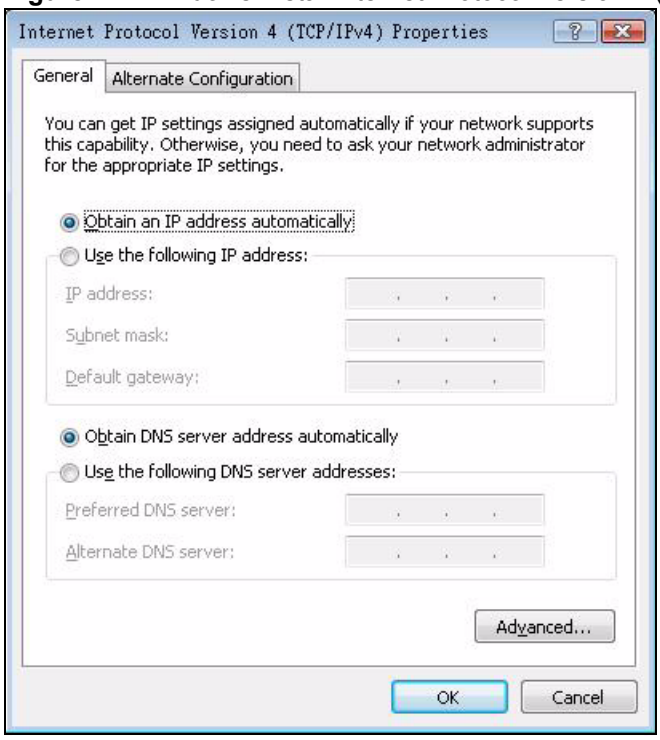
6 Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

Figure 46 Windows Vista: Local Area Connection Properties



7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens (the **General tab**).
- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

Figure 47 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties

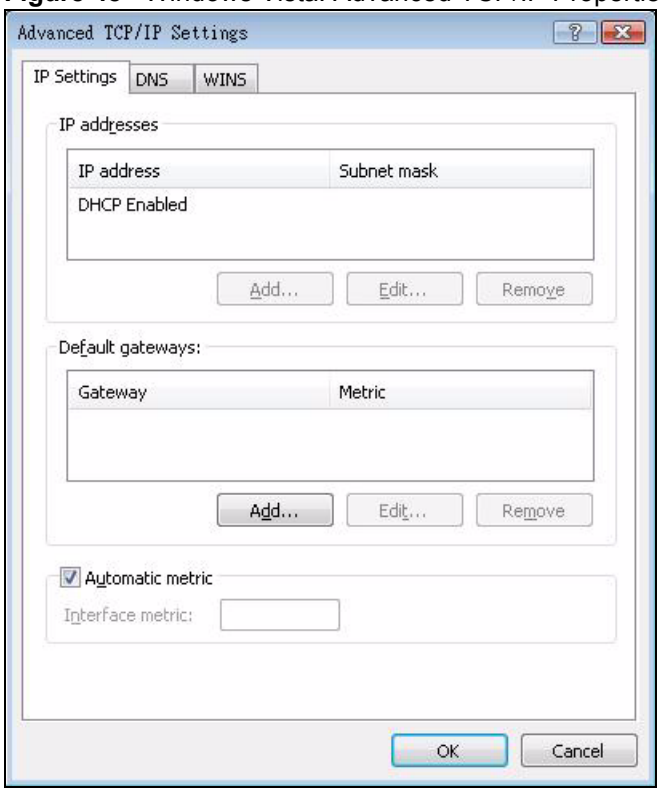


8 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

Figure 48 Windows Vista: Advanced TCP/IP Properties

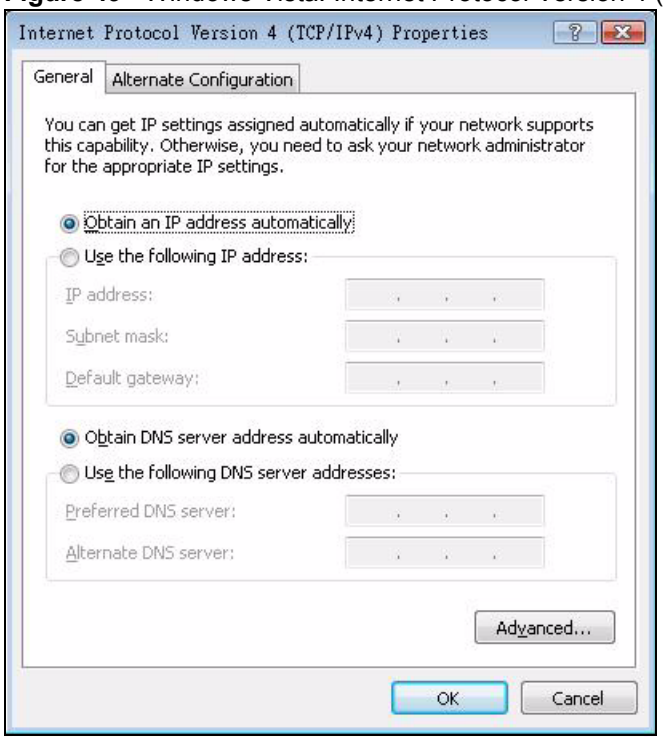


9 In the **Internet Protocol Version 4 (TCP/IPv4) Properties** window, (the **General tab**):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 49 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties



10 Click **OK** to close the **Internet Protocol Version 4 (TCP/IPv4) Properties** window.

11 Click **Close** to close the **Local Area Connection Properties** window.

12 Close the **Network Connections** window.

13 Turn on your NXC-8160 and restart your computer (if prompted).

Verifying Settings

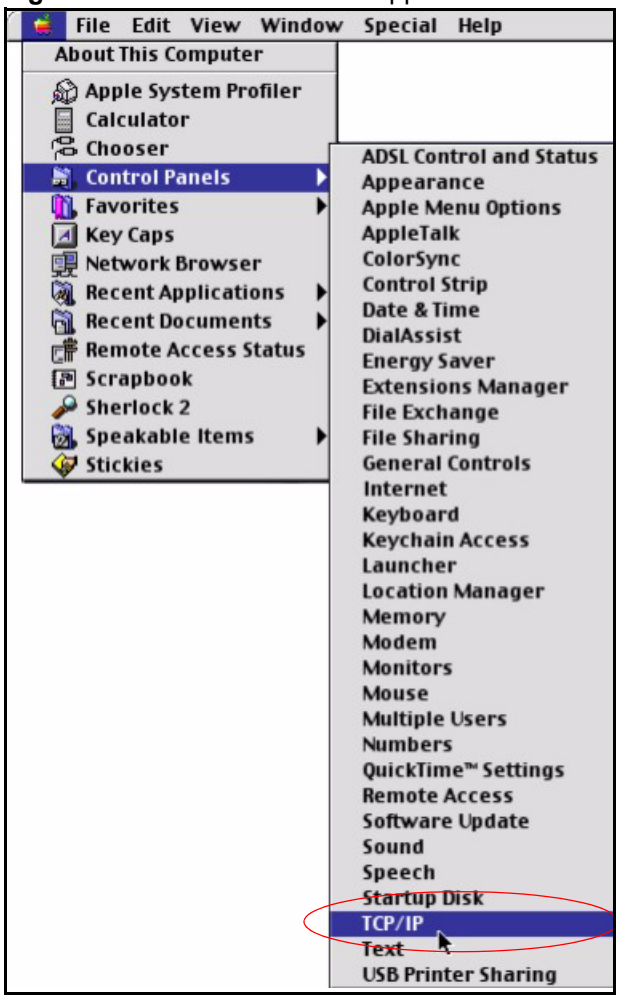
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

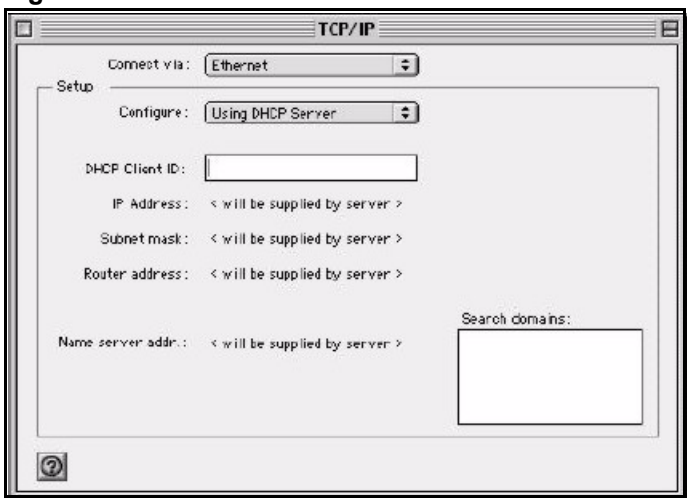
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 50 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 51 Macintosh OS 8/9: TCP/IP



3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.

- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your NXC-8160 in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your NXC-8160 and restart your computer (if prompted).

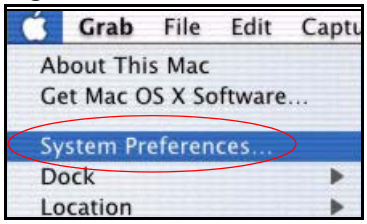
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 52 Macintosh OS X: Apple Menu

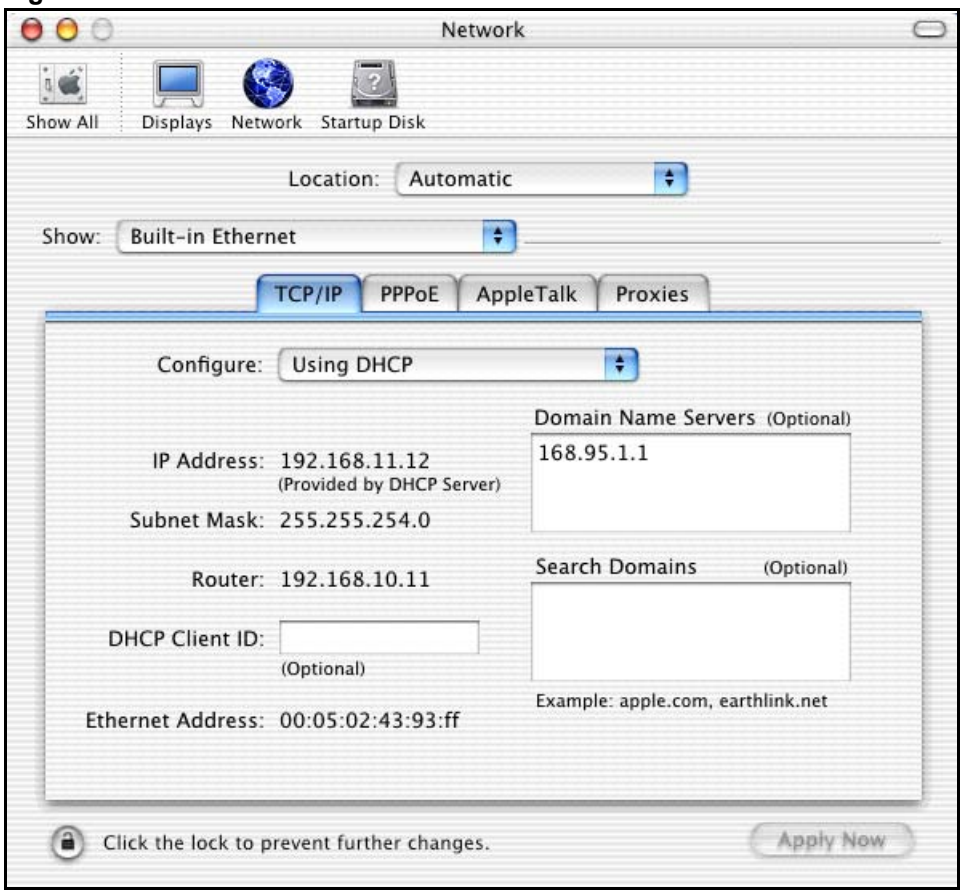


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 53 Macintosh OS X: Network



4 For statically assigned settings, do the following:
   - From the **Configure** box, select **Manually**.
   - Type your IP address in the **IP Address** box.
   - Type your subnet mask in the **Subnet mask** box.
   - Type the IP address of your NXC-8160 in the **Router address** box.
5 Click **Apply Now** and close the window.
6 Turn on your NXC-8160 and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

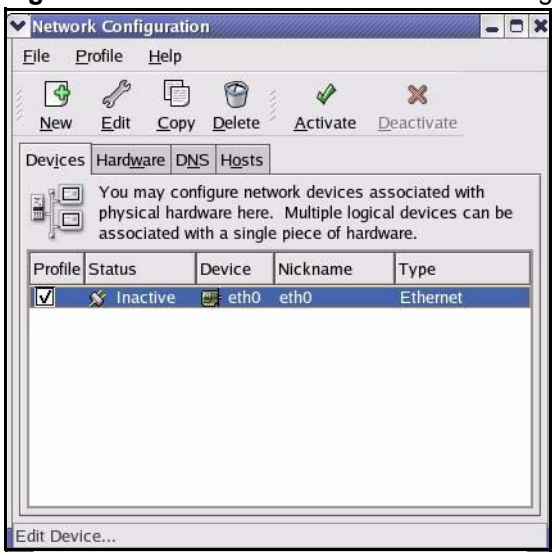
Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 54 Red Hat 9.0: KDE: Network Configuration: Devices



2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

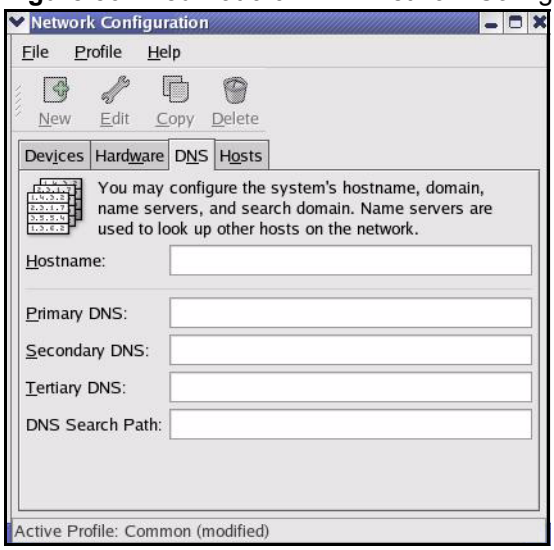
Figure 55 Red Hat 9.0: KDE: Ethernet Device: General

- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

Figure 56 Red Hat 9.0: KDE: Network Configuration: DNS



5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens.**

Figure 57 Red Hat 9.0: KDE: Network Configuration: Activate

7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **`dhcp`** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 58 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **static** in the BOOTPROTO= field. Type IPADDR= followed by the IP address (in dotted decimal notation) and type NETMASK= followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 59 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2. If you know your DNS server IP address(es), enter the DNS server information in the resolv.conf file in the /etc directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 60 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3. After you edit and save the configuration files, you must restart the network card. Enter ./network restart in the /etc/rc.d/init.d directory. The following figure shows an example.

Figure 61 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                [OK]
Shutting down loopback interface:            [OK]
Setting network parameters:                  [OK]
Bringing up loopback interface:              [OK]
Bringing up interface eth0:                  [OK]
```

Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 62 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

B

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

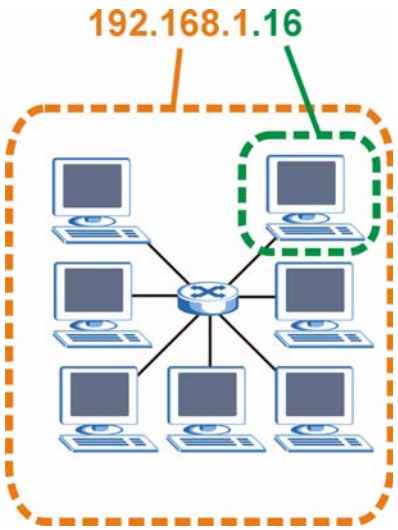
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 63 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 30 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 31 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 32 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} - 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 33 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128

Table 33 Alternative Subnet Mask Notation (continued)

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

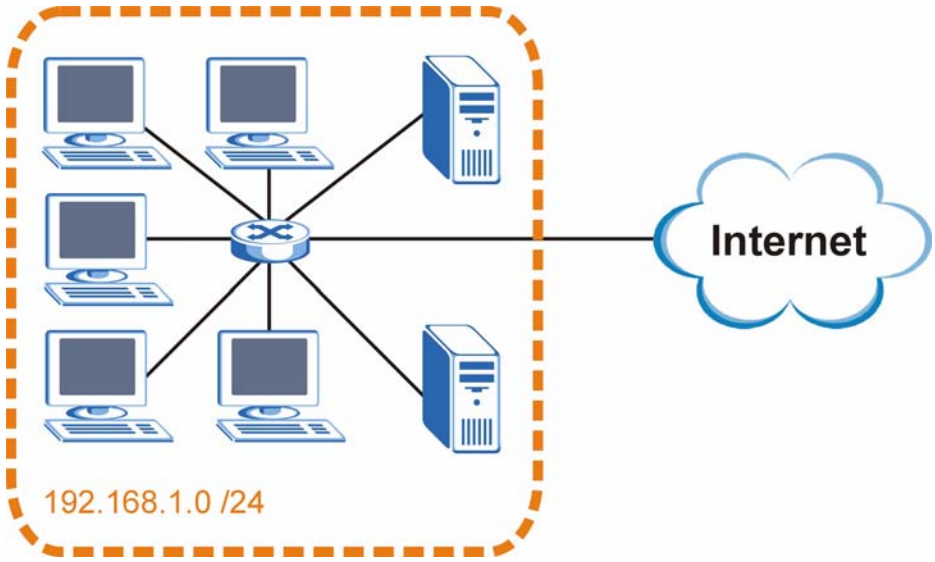
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of $2^8 - 2$ or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 64 Subnetting Example: Before Subnetting

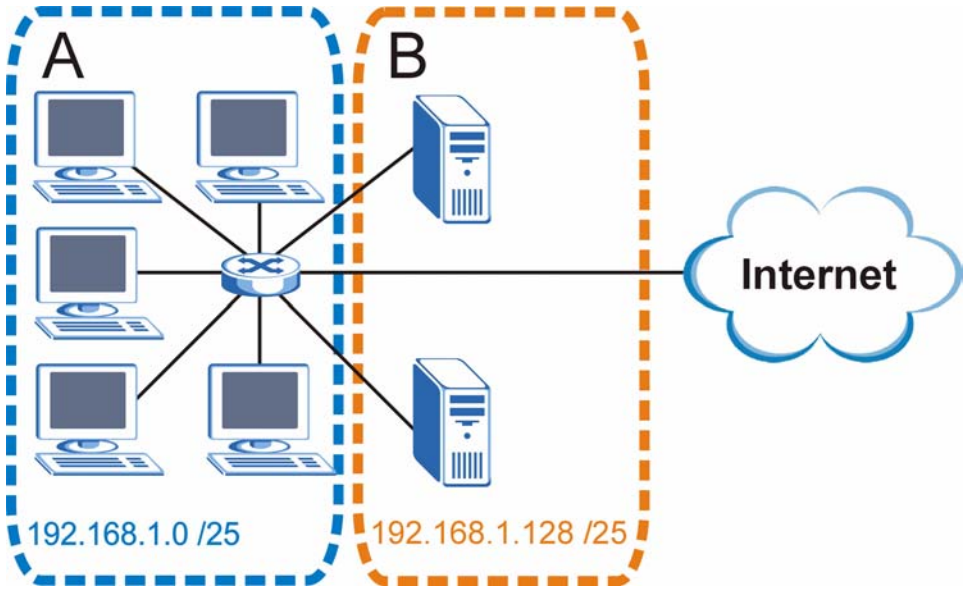


You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The "borrowed" host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 65 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 34 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 35 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 36 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 37 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 38 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127

Table 38 Eight Subnets (continued)

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 39 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 40 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6

Table 40 16-bit Network Number Subnet Planning (continued)

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the NXC-8160.

Once you have decided on the network number, pick an IP address for your NXC-8160 that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your NXC-8160 will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the NXC-8160 unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

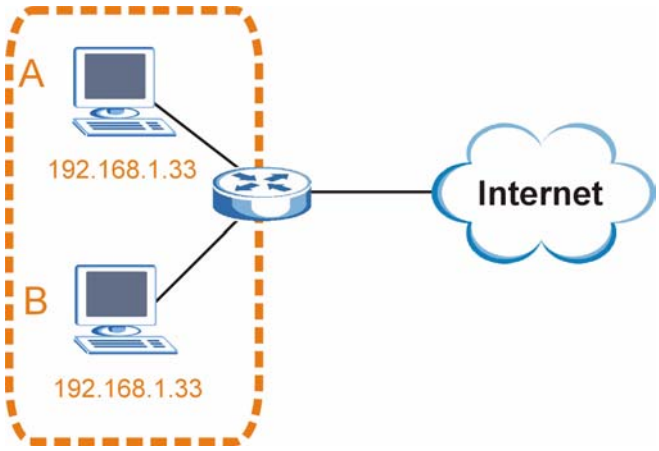
IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

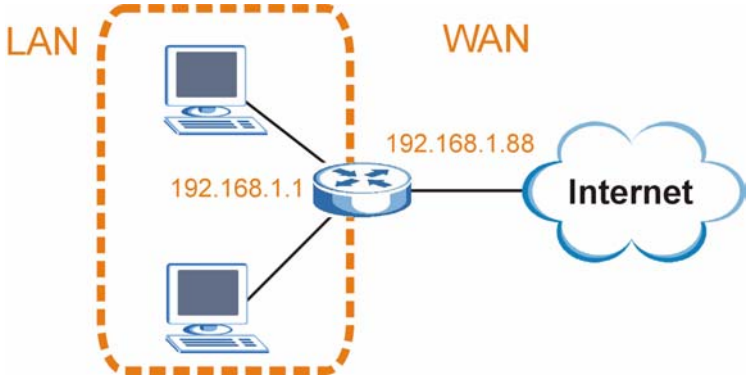
Figure 66 Conflicting Computer IP Addresses Example



Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

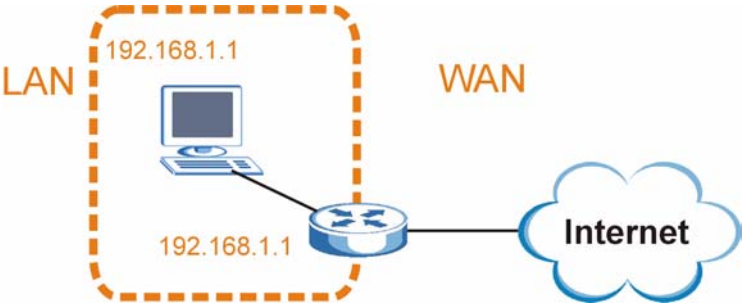
Figure 67 Conflicting Computer IP Addresses Example



Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 68 Conflicting Computer and Router IP Addresses Example



C

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

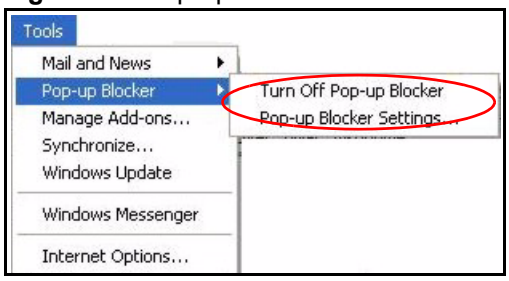
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 69 Pop-up Blocker

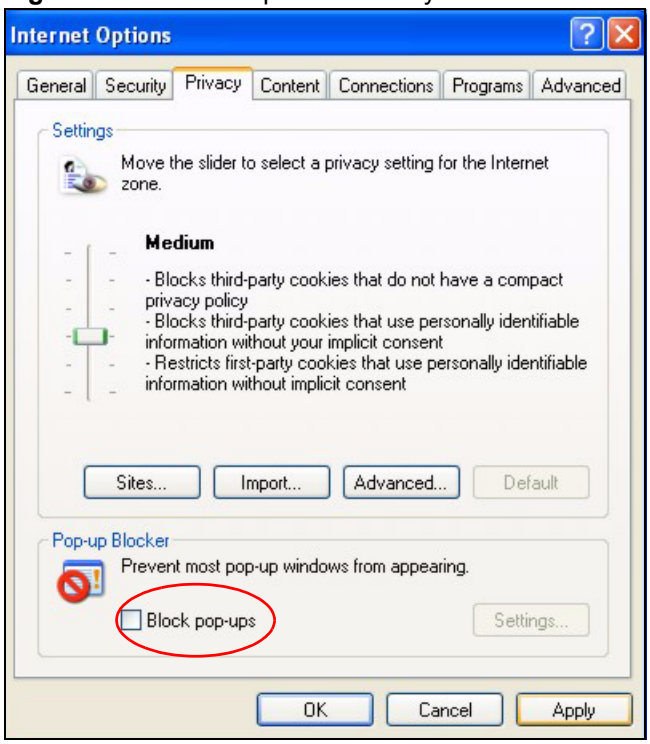


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 70 Internet Options: Privacy



3 Click **Apply** to save this setting.

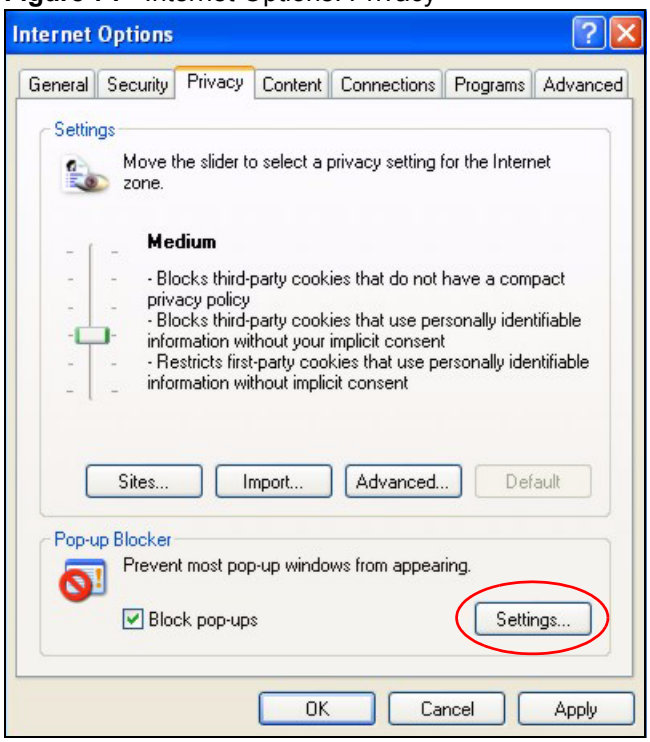
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

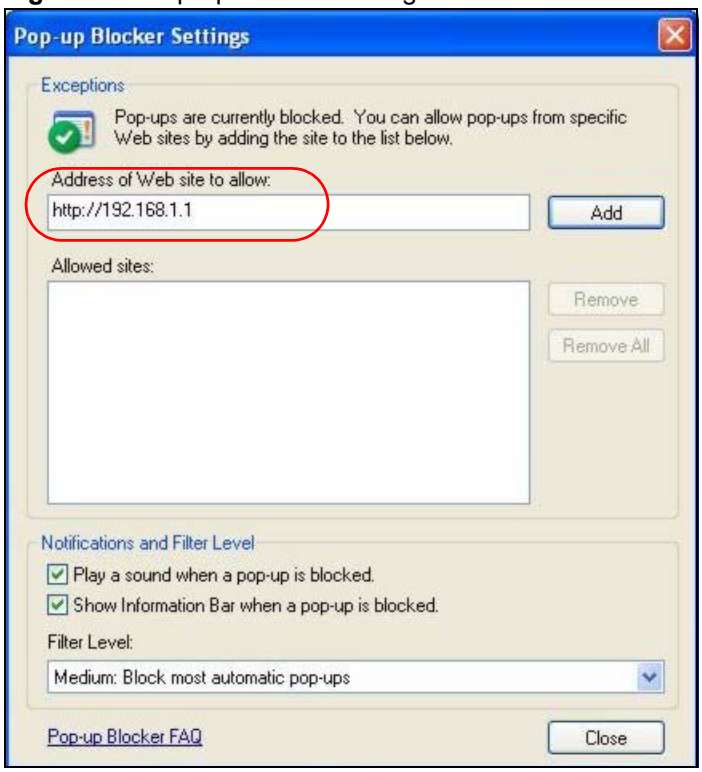
Figure 71 Internet Options: Privacy



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 72 Pop-up Blocker Settings



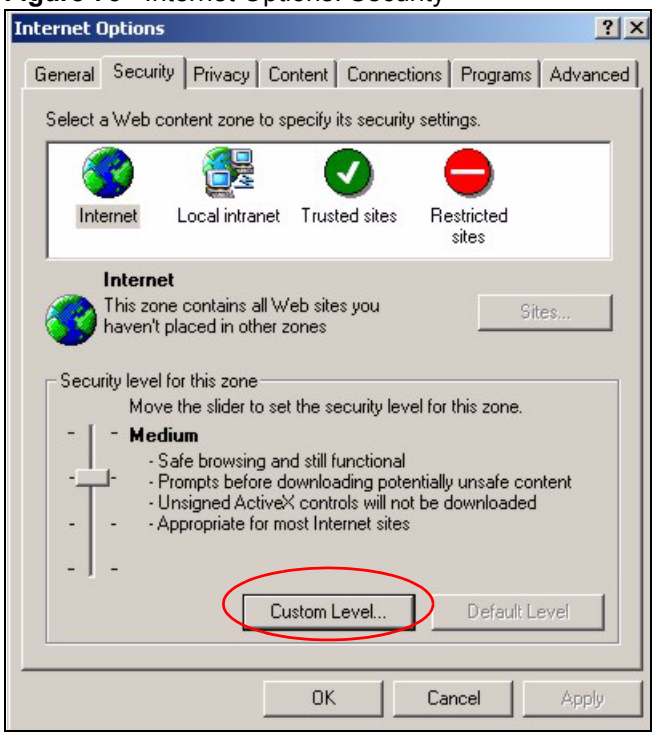
5 Click **Close** to return to the **Privacy** screen.
6 Click **Apply** to save this setting.

JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

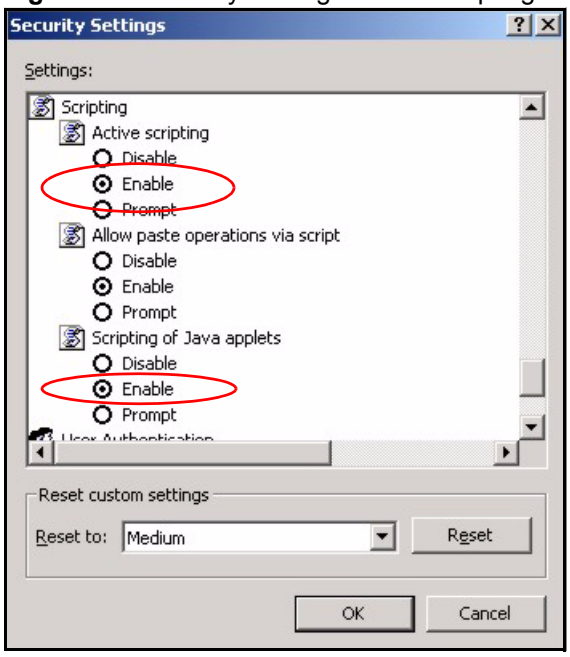
1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 73 Internet Options: Security



2 Click the **Custom Level...** button.
3 Scroll down to **Scripting**.
4 Under **Active scripting** make sure that **Enable** is selected (the default).
5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
6 Click **OK** to close the window.

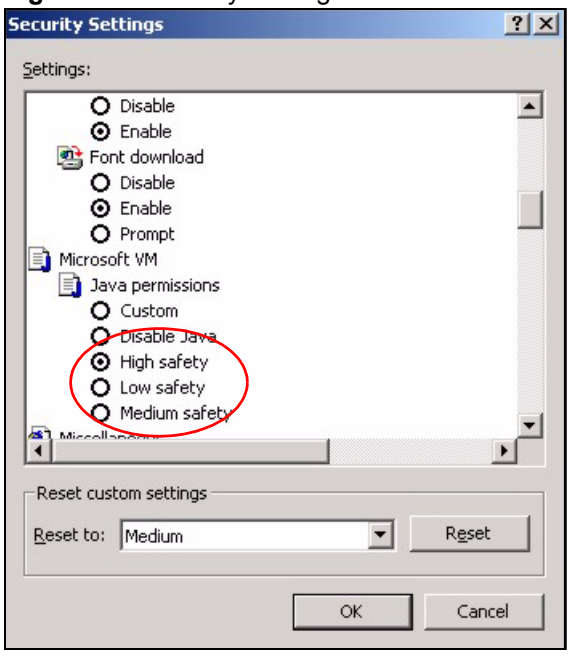
Figure 74 Security Settings - Java Scripting



Java Permissions

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.
2. Click the **Custom Level...** button.
3. Scroll down to **Microsoft VM**.
4. Under **Java permissions** make sure that a safety level is selected.
5. Click **OK** to close the window.

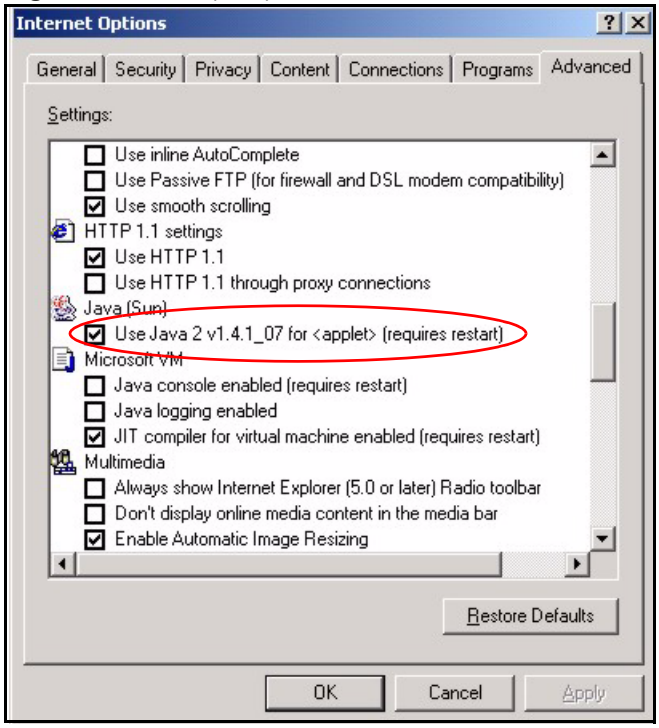
Figure 75 Security Settings - Java



JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.
2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
3 Click **OK** to close the window.

Figure 76 Java (Sun)

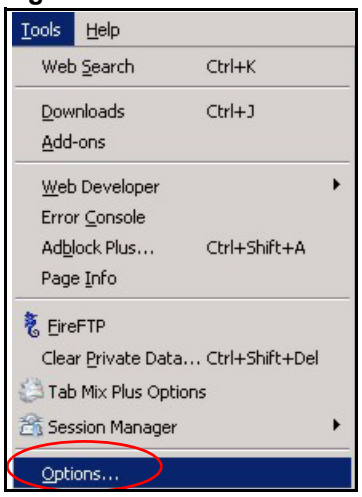


Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

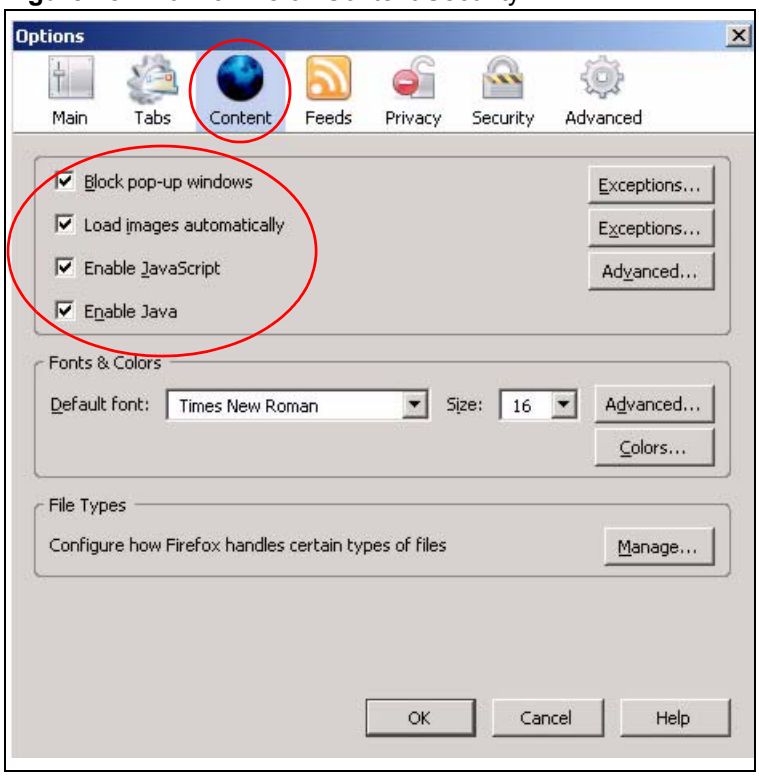
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 77 Mozilla Firefox: Tools > Options



Click **Content**.to show the screen below. Select the check boxes as shown in the following screen.

Figure 78 Mozilla Firefox Content Security



D

Wireless LANs

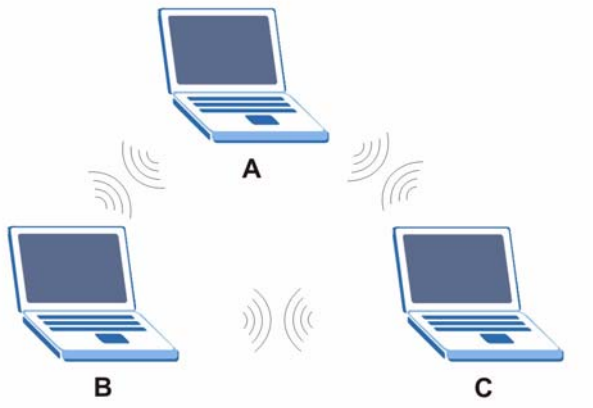
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 79 Peer-to-Peer Communication in an Ad-hoc Network

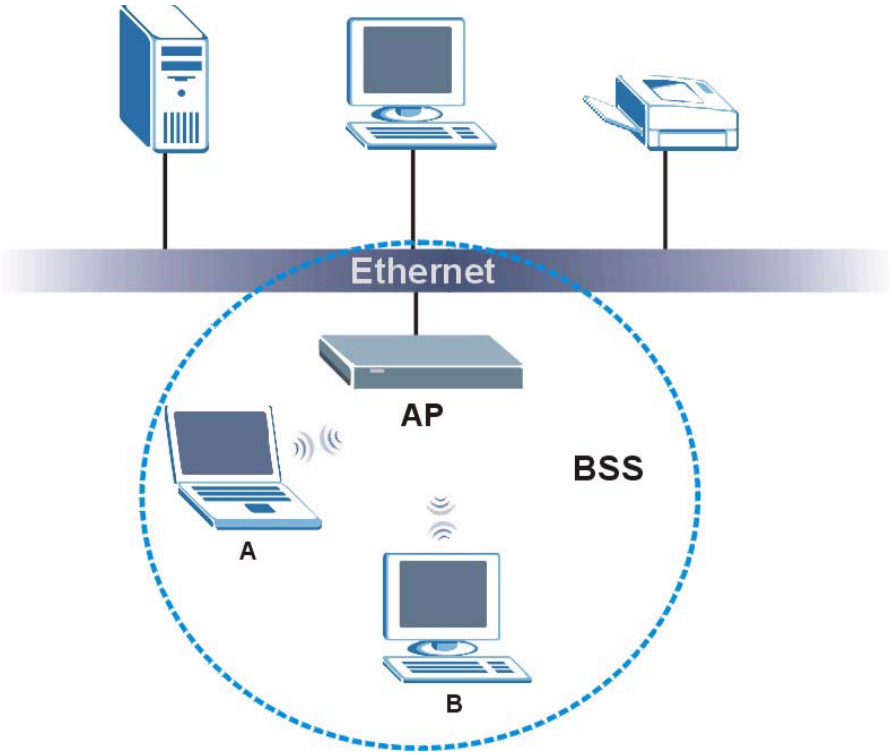


BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 80 Basic Service Set



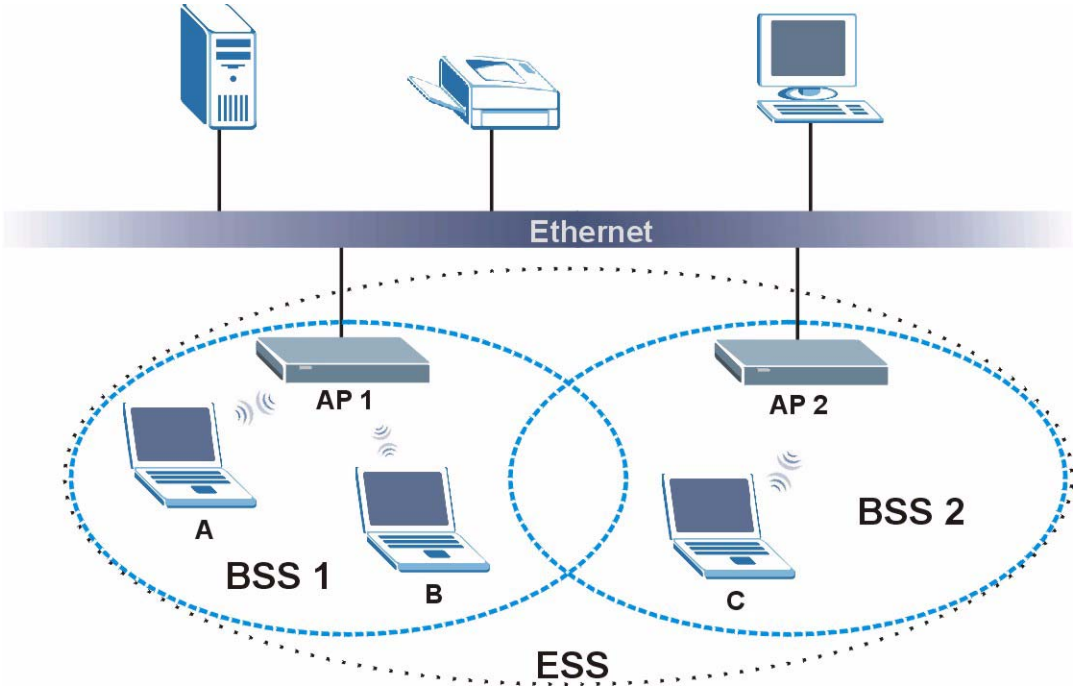
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 81 Infrastructure WLAN



Channel

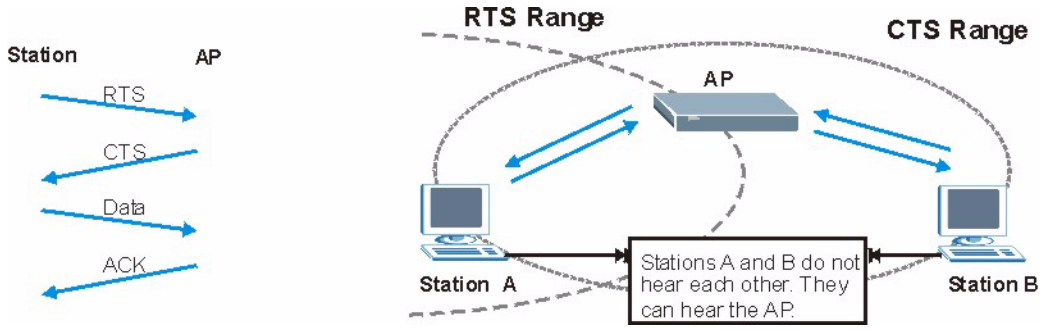
A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 82 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the NXC-8160 uses long preamble.

The wireless devices MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 41 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the NXC-8160 are data encryption, wireless client authentication, restricting access by device MAC address and hiding the NXC-8160 identity.

The following figure shows the relative effectiveness of these wireless security methods available on your NXC-8160.

Table 42 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

You must enable the same wireless security settings on the NXC-8160 and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication
  Determines the identity of the users.
- Authorization

Determines the network services available to authenticated users once they are connected to the network.

- Accounting
  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request
  Sent by an access point requesting authentication.
- Access-Reject
  Sent by a RADIUS server rejecting access.
- Access-Accept
  Sent by a RADIUS server allowing access.
- Access-Challenge
  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request
  Sent by the access point requesting accounting.
- Accounting-Response
  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 43 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

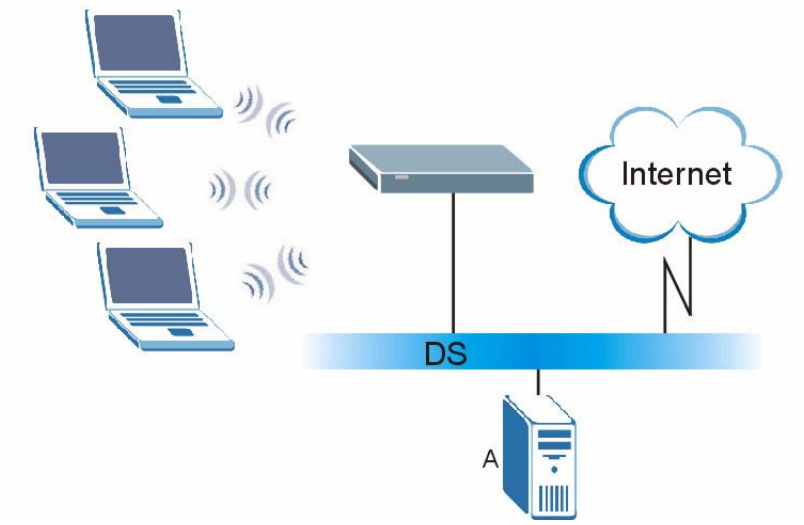
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.
4. The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 83 WPA(2) with RADIUS Application Example



WPA(2)-PSK Application Example

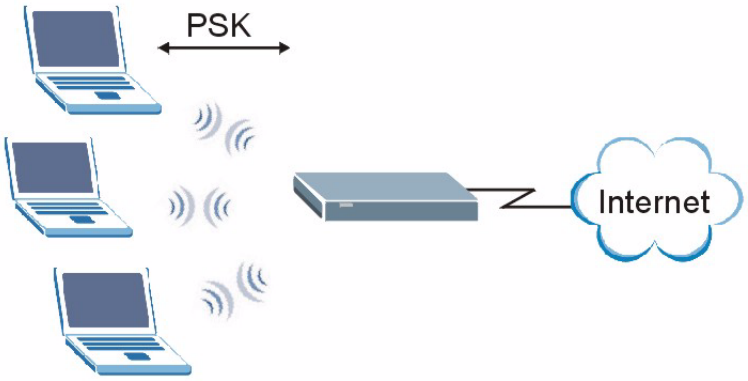
A WPA(2)-PSK application looks as follows.

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).
2. The AP checks each wireless client's password and allows it to join the network only if the password matches.

3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 84 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 44 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

E

Legal Information

Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- For operation within 5.15 ~ 5.25GHz frequency range, it is restricted to indoor environment.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意 !

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

在 5250MHz~5350MHz 頻帶內操作之無線資訊傳輸設備，限於室內使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz and 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Customer Support

Please have the following information ready when you contact customer support.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

"+" is the (prefix) number you dial to make an international telephone call.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com, www.europe.zyxel.com
- FTP: ftp.zyxel.com, ftp.europe.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- FTP: ftp.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350

- Fax: +420-241-091-359
- Web: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

North America

- Support E-mail: support@zyxel.com
- Sales E-mail: sales@zyxel.com
- Telephone: +1-800-255-4101, +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.us.zyxel.com
- FTP: ftp.us.zyxel.com

- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategry #03-28, Singapore 609930

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 08707-555779 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- FTP: ftp.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

Index

U

V

W